Software Engineering Institute

Incident Management Capability Metrics Version 0.1

Audrey Dorofee
Georgia Killcrece
Robin Ruefle
Mark Zajicek

April 2007

TECHNICAL REPORT
CMU/SEI-2007-TR-008
ESC-TR-2007-008

CERT Program

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site http://www.sei.cmu.edu/publications/pubweb.html

Table of Contents

List of Tables and Figures

Abstract

Successful management of incidents that threaten an organization's computer security is a complex endeavor. Frequently an organization's primary focus on the response aspects of security incidents results in its failure to manage incidents beyond simply reacting to threatening events.

The metrics presented in this document are intended to provide a baseline or benchmark of incident management practices. The incident management functions—provided in a series of questions and indicators—define the actual benchmark. The questions explore different aspects of incident management activities for protecting, defending, and sustaining an organization's computing environment in addition to conducting appropriate response actions. This benchmark can be used by an organization to assess how its current incident management capability is defined, managed, measured, and improved. This will help assure the system owners, data owners, and operators that their incident management services are being delivered with a high standard of quality and success, and within acceptable levels of risk.

1 Introduction

1.1 ABOUT THIS REPORT: A BENCHMARK

The Software Engineering Institute is transitioning a method that can be used to evaluate and improve an organization's capability for managing computer security incidents. This set of generic incident management capability metrics leverages earlier work created by the U.S. Department of Defense (DoD) Certification and Accreditation of Computer Network Defense Service Providers (CNDSP) and the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) Federal Computer Network Defense (CND) Metrics. Note that neither of these sets of metrics are (as of the writing of this document) publicly available.

There are many aspects to successfully managing computer security incidents within an organization. Frequently, the primary focus is on the response aspects of computer security incidents and, as a result, the organization fails to adequately consider that there is more to incident management than just responding when a threatening event occurs.

The metrics provided in this document are being published to provide a baseline or benchmark of incident management practices. The incident management functions—provided in a series of questions and indicators—define the actual benchmark.

This benchmark can be used by an organization to assess how its current incident management capability is defined, managed, measured, and improved. This will help assure the system owners, data owners, and operators that their incident management services are being delivered with a high standard of quality, success, and within acceptable levels of risk.

A companion evaluation method will also be published to provide a structured methodology that can be used to guide a practitioner through the process for evaluating an incident management capability.

1.2 WHAT ARE THESE METRICS?

As mentioned above, the metrics are questions that can be used to benchmark or evaluate an incident management capability. Each function or service within the capability has a set of goals, tasks, and activities (that is, a mission of its own) that must be completed to support the overall strategic mission of the organization. The questions explore different aspects of incident management activities for protecting, defending, and sustaining an organization's computing environment in addition to conducting appropriate response actions.

Indicators, included with the metrics questions, are used by an evaluator or practitioner to determine whether a metric has successfully been achieved. The results from an evaluation can help an organization in determining the maturity of their capability, independent of the type of organization (a commercial organization, an academic institution, or a government entity, etc.).

A complete list of the questions is provided in the Appendix.

1.3 WHAT WE MEAN BY INCIDENT MANAGEMENT CAPABILITY

An incident management capability is instantiated in a set of services considered essential to protecting, defending, and sustaining an organization's computing environment, in addition to conducting appropriate response actions. Such services can be provided internally by security or network operators, outsourced to managed security service providers (MSSPs), or they can also be provided and managed by a computer security incident response team (CSIRT). Note that we recognize that it may not always be the CSIRT that performs an incident management activity. However, for the sake of simplicity, the term *incident management personnel* is generally used in this document to represent the groups (or individuals) performing these activities. The terms *constituents* and *constituency* are used to indicate those who are receiving the services provided by whoever is performing incident management activities.

Table 1 provides an overview of the four major function categories—activities conducted in the Protect, Detect, Respond, and Sustain categories. Each category contains a range of subcategories with a set of one or more functions. Each function includes a question about the performance of that function and several indicators that essentially describe the activities leading to adequate performance of that function.

Within the four major function categories, each function is assigned a priority:

- Priority I functions are critical services that a CSIRT or incident management capability should provide.
- Priority II functions are the next most important services. These focus on traditional operational concerns.
- Priority III and Priority IV functions constitute the remaining questions. They represent additional best practices that support operational effectiveness and quality.

Table 1: Function Categories

PROTECT	DETECT	RESPOND	SUSTAIN
• Risk Assessment Support • Malware Protection Support • CND Operational Exercises • Constituent Protection Support and Training • Information Assurance/ Vulnerability Management	• Network Security Monitoring • Indicators, Warning, and Situational Awareness	• Incident Reporting • Incident Response • Incident Analysis	• MOU[1]s and Contracts • Project/Program Management • CND Technology Development, Evaluation, and Implementation • Personnel • Security Administration • CND Information Systems • Threat Level Implementation

[1] MOU stands for Memorandum of Understanding.

1.4 OVERVIEW OF THE MAJOR CATEGORIES

The next few paragraphs will provide an overview of each of the major categories: Protect, Detect, Respond, and Sustain. In each of these categories, the organization must have defined procedures and methods to perform the function; the staff with the requisite knowledge, skills, and abilities (KSAs) to perform the tasks and activities; and the infrastructure with appropriate tools, techniques, equipment, and methodologies to support that work.

1.4.1 Protect

The Protect process relates to actions taken to prevent attacks from happening and mitigate the impact of those that do occur.

Preventative actions secure and fortify systems and networks, which helps decrease the potential for successful attacks against the organization's infrastructure. Such steps can include

- implementing defense-in-depth and other best security practices to ensure systems and networks are designed, configured, and implemented in a secure fashion
- performing security audits, vulnerability assessments, and other infrastructure evaluations to identify and address any weaknesses or exposure before they are successfully exploited
- collecting information on new risks and threats and evaluating their impact on the organization

Mitigation involves making changes in the enterprise infrastructure to contain, eradicate, or fix actual or potential malicious activity. Such actions might include

- making changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure
- updating IDS or anti-virus signatures to identify and contain new threats
- installing patches for vulnerable software

Changes to the infrastructure may also be made, based on the process improvement changes and lessons learned that result from a postmortem review done after an incident has been handled. These types of changes are made to ensure that incidents do not happen again or that similar incidents do not occur.

1.4.2 Detect

In the Detect process, information about current events, potential incidents, vulnerabilities, or other computer security or incident management information is gathered both proactively and reactively. In reactive detection, information is received from internal or external sources in the form of reports or notifications. Proactive detection requires actions by the designated staff to identify suspicious activity through monitoring and analysis of a variety of logging results, situational awareness, and evaluation of warnings about situations that can adversely affect the organization's successful operations.

1.4.3 Respond

The Respond process includes the steps taken to analyze, resolve, or mitigate an event or incident. Such actions are targeted at understanding what has happened and what needs to be done to enable the organization to resume operations as soon as possible or to continue to operate while dealing with threats, attacks, and vulnerabilities. Respond steps can include

- analysis of incident impact, scope, and trends
- collection of computer forensics evidence, following chain of custody practices
- additional technical analysis related to malicious code or computer forensics analysis
- notification to stakeholders and involved parties of incident status and corresponding response steps
- development and release of alerts, advisories, bulletins, or other technical documents
- coordination of response actions across the enterprise and with other involved internal and external parties, such as executive management, human resources, IT and telecommunication groups, operations and business function groups, public relations, legal counsel, law enforcement, internet service providers, software and hardware vendors, or other CSIRTs and security teams
- verification and follow-up to ensure response actions were correctly implemented and that the incident has been appropriately handled or contained

1.4.4 Sustain

The Sustain process focuses on maintaining and improving the CSIRT or incident management capability, itself. It involves ensuring that

- the capability is appropriately funded
- incident management staff are properly trained
- infrastructure and equipment are adequate to support the incident management services and mission
- appropriate controls, guidelines, and regulatory requirements are followed to securely maintain, update, and monitor the infrastructure

Information and lessons learned from the Protect, Detect, and Respond processes are identified and analyzed to help determine improvements for the incident management operational processes.

1.5 INTENDED AUDIENCE

This document is intended for individuals and organizations who want to baseline their incident management functions to identify strengths and weaknesses and improve their incident management capability. The guidance is provided to help an individual practitioner or team understand the application of these questions against a series of baseline requirements and indicators that can lead to an evaluation of an effective incident management capability.

2 Explanation of the Structure

The structure for each incident management function provides two basic sets of information.

- explanatory information and scoring guidance—additional information explaining the significance of the function and how to evaluate the performance of that function
- the function itself, presented in a table with a main question, and a more detailed set of indicators that can be used by the evaluator to assess the performance of the function

Each function also includes a set of cross-references to selected regulations or guidance: Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) publications, and best practices.

As stated previously, each function includes indicators to evaluate the performance of that function. Indicators that must be met have an added "required" label (indicated by the placement of [R] at the end of the statement). These required items are best practices for ensuring that an effective capability exists for incident management.

The indicators cover six groups:

- *prerequisites* that must be met before this function can be performed, or be performed adequately
- *controls* that are available or exist that direct the proper execution of the activities
- *activities* that are performed as part of this function (and could be observed by an evaluator)
- *supporting mechanisms* that are needed for adequate execution of activities
- *artifacts* that result from or support the activities and can be observed by an evaluator to verify execution of activities
- *quality* indicators that measure effectiveness, completeness, usefulness and other quality aspects of the activities

An example of a function table is shown in Figure 1. To help the evaluator use the tables, the following list explains how the information for each function is organized. Reading the table from left to right, the fields are

1. major function category and number – protect, for example
2. function subcategory and number – risk assessment support, for example
3. function reference number – represents major category, subcategory, and specific function, for example, 1.1.1
4. question – the function that is being evaluated
5. priority – I through IV (where Priority I is the most important)
6. Not Observed – used to indicate situations where function was not observed during the evaluation

7. Not Applicable – in those cases where this may apply[2], the function is excluded from the scoring
8. Yes statement – defining what is required to score this question as having been fully met
9. Partial statement – defining what is required to score this question as having been partially met (only present for Priorities II, III, and IV)
10. Score – value based on evaluation results
    - For Priority I functions, the scoring selection is "Yes" or "No"
    - For Priority II-IV, the scoring selections are "Yes", "Partial", or "No"
11. Indicators – the items, actions, or criteria the evaluators can see or examine during the evaluation to help them determine whether the metric is being met (refer to additional details in guidance and scoring requirements). Those indicators that are required for a [Yes] score are marked with a [R]
12. References – standards, guidelines, or regulations relating to this function, including a placeholder for organization-specific references

<table>
<tr><td colspan="6">Incident Management Capability Functions</td></tr>
<tr><td colspan="6">{1} Major function category</td></tr>
<tr><td colspan="6">{2} Function subcategory</td></tr>
<tr><td>{3} Function reference #</td><td colspan="3">{4} Question</td><td colspan="2">{5} Priority</td></tr>
<tr><td rowspan="2">{6}
Not observed
❑</td><td rowspan="2">{7}
Not applicable
❑</td><td>{8}
Yes</td><td>▪ statement representing Yes answer for question</td><td rowspan="2">{10}
Score
Y ❑ P ❑ N ❑</td><td></td></tr>
<tr><td>{9}
Partial</td><td>▪ statement representing Partial answer for question</td><td></td></tr>
<tr><td colspan="6">Prerequisites ❑
Controls ❑
Activity ❑
Supporting Mechanisms ❑
Artifacts ❑
Quality ❑
{11} {INDICATORS}</td></tr>
<tr><td colspan="6">{12} Regulatory References:</td></tr>
<tr><td colspan="6">{12} Guidance References:</td></tr>
<tr><td colspan="6">{12} Internal Organization References:</td></tr>
</table>

Figure 1: Standard Format for an Incident Management Capability Function Table

[2] Note that the guidance and scoring description provides additional information about Not Applicable responses.

3 Using these Metrics to Evaluate the Incident Management Capability of an Organization

This section provides an overview of how the metrics can be used to assess and improve an organization's incident management capability. A complete evaluation method description for using these metrics by an expert team will be documented and released in the future. It is possible to use these metrics for a broad range of evaluations. For example, the entire set of metrics can be used to evaluate an organization's entire incident management capability. A subset could be used to more narrowly focus on only the specific responsibilities of an actual CSIRT or a security service provider. The extent or scope of the evaluation is determined early in the process, based on the goals of the organization or sponsor of the evaluation. The assumption for this section is that the entire incident management capability is being evaluated. A narrower scope would simply use fewer metrics and evaluate fewer groups.

Incident management, as a complete capability, includes activities that may be performed by a CSIRT or by other groups across an organization. There may be several groups, each with some distinct or overlapping responsibilities, that support management of cyber security events and incidents. In this latter case, applying these metrics only against the designated CSIRT may result in an inaccurate or very limited view of the organization's total ability to effectively manage cyber security incidents. An evaluation should consider all groups performing incident management activities in order to produce accurate results.

An evaluation using these metrics generally requires the following tasks:

- Identify the groups involved in incident management and allocate their functions to the groups (from the Protect, Detect, Respond, and Sustain categories).
- Assess each group.
- Look at the results and decide whether the group is effectively performing its functions or identify what to improve.
- Determine what to do about groups that cannot be assessed.

3.1 IDENTIFY THE GROUPS INVOLVED IN INCIDENT MANAGEMENT AND ALLOCATE THE FUNCTIONS

There are many techniques for identifying the groups involved in incident management. One technique would use a benchmark for incident management, such as that described by Alberts [Alberts 2004]. By comparing the organization to this process model of incident management activities, all of the groups performing such activities can be identified. Another alternative would be to use some form of work process modeling [Sharp 2001] to map out all of the groups and interfaces associated with incident management activities. Once the groups and activities have been identified, functions can be allocated to each group (e.g., allocate Detect functions to the groups performing network monitoring).

3.2 ASSESS EACH GROUP

The simplest way to assess each group against its functions is to conduct interviews or group discussions and ask the assembled individuals about each function that is applicable to their group. Artifacts related to the functions can be requested and reviewed, and where necessary, activities can be observed. The scoring guidance (in Section 4 and with each metric) and the indicators included with the function provide help by listing prerequisites that are needed, activities that are performed, supporting mechanisms that may be in place to help do the work, or physical artifacts (forms, templates, lists, etc.) that can be examined for completeness and currency. To further assist the evaluator, as mentioned earlier, some indicators are designated as required [R]. These indicators must be met to obtain a successful or passing score for that function.

Priority I metrics will be scored either as a Yes or No. Priority II, III, and IV metrics can obtain scores of either Yes, Partial or No. For further delineation of the results, a five-point scale using Qualified Yes and Qualified No in addition to Yes, Partial and No is also a possibility, although it is not discussed further in this document.[3] It is also possible that the function could be scored either "Not Observed" or "Not Applicable."

"Not Observed" is used when a function cannot be evaluated because the evaluator does not have access to the individuals who can provide the correct answer, or cannot observe that the activity or function was performed. "Not Applicable" is used when the activity is not performed by the organization as part of the incident management processes. The guidance and scoring information preceding each metric provides additional information to help the evaluator in situations where a Not Observed or Not Applicable claim is made.

3.3 LOOK AT THE RESULTS AND DECIDE WHAT TO IMPROVE

The organization, at this point, will have a clear idea of how well it is meeting these metrics with respect to incident management. It will know what its strengths and weaknesses are. To improve the processes, the organization can look at the resulting scores and begin to build a strategy for improvement by building off its strengths. For example, the following questions could be asked:

- Are there any Priority I functions with a score of No?
  - If so, these should be the first candidates for improvement.
- Are there any Priority II, III, IV functions with a score of No?
  - If so, these are the second candidate set for improvement, in Priority order (in other words, improve the Priority II functions first, the Priority IV functions last).
- Are there any Priority II, III, IV functions with a score of Partial?
  - These are the third candidate set for improvement, in Priority order.

Existing strengths can be used to improve weaker areas. For example, if some functions have exceptionally good procedures and policies, use those as a basis for developing policies and

[3] The forthcoming evaluation method document for these metrics will include a detailed discussion of a five-point scale, which can provide a much more refined picture of the state of the organization's incident management capability. This more refined picture provides a better platform of improvement with the greater granularity of the evaluation results.

procedures for functions where they are not as robust or missing. If there is a strong training program for some types of personnel, expand that program to include additional types of training for identified incident management functions that are lacking.

Note that a further review of the results may be needed when considering improvements in the Priority II through Priority IV functions—for example, improving a Priority IV metric from No to Partial might be less critical than improving a Priority II function from Partial to Yes. Each organization will need to make its own determination concerning the order in which to improve scores on any Priority II-IV functions based on a review of the entire set and by considering the changes that are needed, the required resources, the mission, goals, and objectives.

Finally, a common type of improvement for all of the functions can be found by looking at the non-required indicators. This type of improvement goes beyond meeting best practice and considers additional improvements that can build an exceptional incident management capability. Even those functions where required indicators were successfully met can be improved by implementing the non-required indicators.

Ultimately, the end goal for these metrics (or other types of assessments) is to strive for continuous improvement of the processes, so it is also a recommended best practice to periodically re-evaluate to see what new "current" state has been achieved. This could be done on an annual basis or as conditions change (e.g., as new technologies are deployed, the infrastructure changed, or new partnerships or supply chains adopted).

3.4 DETERMINE WHAT TO DO ABOUT GROUPS THAT CANNOT BE ASSESSED

Given the complexities and political realities of some organizations, it may not be possible to meet with some groups or obtain access to certain types of information. At the very least, the interface to that group should be evaluated. The organization can then decide if those groups should be evaluated at a later time, or whether arrangements can be made for those other groups to assess themselves using applicable information from these metrics, and to then provide the results (or feedback) to appropriate individuals. Alternatively, an external or third-party organization can be contracted to perform the evaluation on the relevant groups.

3.5 FINAL THOUGHTS

These metrics are a starting place for identifying improvements. They are not a precisely defined path for every organization to build the perfect incident management capability, but serve as a baseline for determining the effectiveness of teams, based on approaches used by other entities and the experience of the CERT Program in helping organizations build their teams or incident management capabilities. One additional comment on considering the positive or negative impacts can be made. Each function should be examined to consider the relative consequences of "doing" or "not doing" the function or required indicators therein. This can provide elemental insight into whether the result will be a detrimental or unexpected result. Look to the suggested improvements for ideas on enhancing performance or identifying ways to improve. In applying the metrics, use judgment and common sense, respect the budgetary process, and stay abreast of changing regulations and standards in this ever-evolving environment.

Furthermore, there has been no mention of adding up the scores to achieve some predefined threshold that constitutes a "passing" score. The metrics must be tested and used by the

community to determine if scoring ranges would be relevant, accurate, and achievable, and if so, what those ranges would be.

Our goals are to work with the incident response community and others to discuss what constitutes the appropriate threshold scores for a CSIRT or incident management capability. For example, are different "ranges" of thresholds required for different types of teams, such as a corporate team vs. a national team?

One suggested approach for transitioning the metrics has been to release them publicly, encourage adoption, and establish a baseline set of thresholds. These thresholds can slowly increase to "raise the bar" across the different types of CSIRTS for what constitutes a passing score. This approach can also serve as the appropriate driver for continuous improvement in incident management activities. For example, start with some established set of percentages across each Priority (e.g., you would need to successfully perform 75% of the Priority I functions, 60% of the Priority II functions, and so on), then periodically increase the percentages needed to achieve success. Determining how to raise the threshold could be done through regularly scheduled reviews of the metrics themselves to keep them aligned with the current state of the art. These are all future considerations.

For the present these metrics can be used to identify critical weaknesses in the organization's incident management capability and provide insight for where to make practical improvements.

4 General Guidance for Scoring Metrics

This section discusses some issues evaluators need to remember as they are conducting the evaluation. The guidelines addressed here are

- answer the primary function question first
- check completeness and quality of documented policies and procedures
- determine personnel knowledge of procedures and successful training
- identify quality statistics

4.1 ANSWER THE FUNCTION QUESTION FIRST

The function question is what the evaluator is seeking to answer; it is the overarching measure as to whether the activity is being performed. The included indicators provide guidance that assists the evaluators in answering the function question. For example, while the initial answer to the question may be "Yes, we do vulnerability scans," the indicators provide the evaluator with the means of gathering additional supporting information to prove that vulnerability scans are done effectively through documented procedures and training, and that the results of scans are analyzed and passed to appropriate personnel to take action, etc.

As a cautionary note, in evaluating a function, don't forget to get the answer to the question. In most cases the question itself and the statements defining the [Yes] or [Partial] conditions are not repeated specifically under the indicators.

4.2 CHECK COMPLETENESS AND QUALITY OF DOCUMENTED POLICIES AND PROCEDURES

For evaluators, when deciding if documented policies and procedures referenced in the Control indicators are adequate, consider the following:

- Does the policy or procedure adequately address the process, technology, requirements, expected behaviors, or other topic it is supposed to address?
- Do the procedures reflect what is actually done by personnel?
- Are the policies and procedures easily available to personnel?
- Are the policies or procedures being kept up to date? There should be a review and/or revision date or some indication that they are reviewed and changed as needed.[4] Also look for
  - defined process and periodicity for reviewing and revising
  - established criteria for when to review (e.g., change in organization structure, major technology installation)
  - defined roles and responsibilities for review and update

[4] The evaluator should use judgment to determine if a real revision was made or if the date was simply changed to make it look up to date. The evaluator could ask to see specific changes or compare the document to the previous version.

- defined process for communicating changes and revisions throughout relevant parts of organization
- change log history

4.3 DETERMINE PERSONNEL KNOWLEDGE OF PROCEDURES AND SUCCESSFUL TRAINING

The evaluator should be able to determine from discussions with the personnel whether they understand the process (e.g., they are able to intelligently describe it). More importantly, the personnel should be able to easily show how they perform that work (show the forms that they fill in, describe the process by which they take information from an incident report that is displayed and extract information to feed into summary or other organizational or regulatory reports, or demonstrate how they perform analysis on a set of logs, etc.).

Training can range from formal training that has complete packages with materials and dedicated instructors to informal, on-the-job mentoring by more senior personnel. The evaluator is seeking to determine whether training is provided, that it is sufficient to meet the needs of organization, and, as shown in the Quality indicators, that the personnel are knowledgeable and perform the procedures consistently.

The observation of personnel performing the tasks is a further indication of the maturity of the operations and training that has been provided. For example, observation can show that personnel know the following:

- how to discuss the process with a level of understanding that supports knowledge of their functions with regard to the activities being observed
- where reports or data are archived
- what types of information are contained in reports or alerts or other documents and products
- where procedures, policy, or guidance documents are kept and how to access them if needed
- how to use the tools that support the functions

4.4 IDENTIFY QUALITY STATISTICS

Evaluating quality indicators can be accomplished in many ways. At the most basic, discussions with personnel can be used to determine if they have anecdotal or quality assurance reports showing the percentage or numbers of items they produce that meet quality measures (and what those measures are). For example, if there are reports or references to meeting a general or specific percentage for usefulness to constituent, continue to inquire how "usefulness" is defined. It is easy to say that all response guidance is useful but if "useful" is not defined or the wrong people are asked, then a very subjective and inaccurate picture could result.

It's worth noting here that because *quality* measures or statistics are not necessarily in common use in the security field, it may be difficult to obtain such information, and what is available may not be very accurate or meaningful. In many cases constituents are polled or surveyed using open-ended or vague questions that fail to accurately obtain the intended results. For example, while it may be easy to recognize that the guidance provided to constituents is clear and easy to understand, it may be difficult to measure whether the constituents actually *follow* the guidance provided.

Evaluators should use their own judgment when it comes to looking at any quality statistics or reports in terms of the definition of the quality measures, the applicability of the measures, the means of collecting them, analysis techniques, and what happens with the reports once they have been obtained—reporting for the sake of reporting is not as effective as using the results from such reports as input into appropriate follow-on actions or as part of an improvement process.

5 The Incident Management Capability Metrics

The remainder of this document contains Version 0.1 of the metrics. There are five sections, representing the four main categories of metrics as well as an additional category at the beginning for common metrics. These sections are

- Common: Section 0 of the metrics
- Protect: Section 1 of the metrics
- Detect: Section 2 of the metrics
- Respond: Section 3 of the metrics
- Sustain: Section 4 of the metrics

These metrics are a work in progress, and so there may be places where "To Be Determined" or TBD is used a placeholder. In some cases, there could be multiple answers to a TBD, which could have varying degrees of complexity, depending on the type of organization and maturity of the incident management capability. As a result, we have left these placeholders to encourage users of these metrics to consider what response is most appropriate.

COMMON: SECTION 0 OF INCIDENT MANAGEMENT CAPABILITY METRICS

There are four main categories of functions: Protect, Detect, Respond, and Sustain. However, there also appear to be functions that are "common" to all or most of the categories. At this point, there is only one common function that we have included. From our research and interactions with customers, as well as discussions with teams over the years, the one interface that continues to be critical is communications. It can often be traced to the cause of a delay or failure in action. It is a key success factor for an incident management capability to examine its communications requirements and pathways, to ensure they are clearly defined, and to exercise diligence in ensuring they are effective, efficient, and understood by those involved in those communications.

The *organizational interface metric* is a common function that is focused on the interfaces between any groups performing incident management activities. An interface is any communication, exchange of information, or work that occurs between two groups. The interface output from one group could be electronic data, email, a conversation, a report, a request for assistance, automated distribution of information, logs, or analyses that serve as input into the other group.

Note that this interface function is a bit unusual because it requires a bidirectional evaluation. When there is an interface between two groups (such as a CSIRT and its constituents, or an Information Security Officer [ISO] and law enforcement) this interface should be asked of *both* sides—for example, it's not only important to know that a CSIRT thinks the interface is working well, the evaluator should ask whether the ISO thinks the interface is working well.

The importance of this interface function is clear when you consider that a CSIRT (or some other group) may need to improve a specific Priority I function that depends entirely upon the successful completion of an activity by another group. If the other group is too busy to make improvements, a CSIRT would be left unable to improve its component piece of the incident management process. If the interface were undefined, undocumented, and unenforceable, then a CSIRT would have no real basis on which to argue for improvement. If the interface were well documented, with clearly defined roles and responsibilities, then a CSIRT would have the grounds to ask management to help enforce the agreement.

As other common functions are identified, they will be added to this section. Other candidates for this section may be, for example, personnel training or policy and procedures management.

0. Common Functions

0.1 Organizational Interfaces

0.1.1 Have well-defined, formal interfaces for conducting organization incident management activities been established and maintained?

This function focuses on the interfaces between the various groups involved in incident management functions, including internal components (e.g., a CSIRT, ISO, or a network administration group) and external groups such as service providers or subcontractors. Interviewing external groups for an evaluation might be difficult. Therefore, it may only be practical to evaluate the organization side of the interface. All interfaces should be identified and discussed, whether informal or formal. The best practice is to have interfaces formalized, but informal interfaces may be all that exist.

Please note: There may be multiple interfaces to evaluate to answer this question, depending upon how many groups are performing incident management activities. The simplest means for evaluating this question is to gather information about the various interfaces and provide a summary answer for how well interfaces, in general, are handled. If the evaluation team decides it is necessary, each interface could be evaluated against this function separately, with an individual score for each interface.

Not applicable – This question is Not Applicable if there is no interface or *need* for an interface between groups within the organization. While an interface may not currently exist, if the need for one is raised during the course of evaluating organizational incident management activities, then the answer to this question can be used by the organization to show that the interface is needed as part of its improvement and that both groups should be involved in refining the interface.

Impact Statement – When interfaces are properly defined and managed, there are no gaps or poorly functioning processes in the flow of any work or information associated with the incident management activities.

Scoring and interpretation guidance – The goal of satisfying this question is to show that the interface is appropriately documented to prevent misunderstandings or incomplete performance and that each side of the interface performs according to requirements. A failing answer to this question applies to all sides of the interface, not to just one group. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory grading of this question [Yes] can be achieved only if all of the required indicators [R] have been met for all of the identified interfaces. A permissible variation for a Yes score would be to determine that some interfaces are critical and check that all required indicators for critical interfaces are met and the majority of the required indicators are met for non-critical interfaces. Note the following:
  - How an interface is documented can vary greatly—from a series of email exchanges between managers to formal contracts. As long as the required aspects are documented and personnel responsible for the interface know about and meet the requirements, the formality of the interface is left to the organization.
  - The evaluator should be able to determine from discussions with personnel whether they know how to properly interface with another group (e.g., by whether they are able to

intelligently describe it). More importantly, personnel should be able to easily show how they perform that work (e.g., show the forms that they fill in, describe the process for providing and receiving inputs and outputs to and from the interface).

- There may be no hard copy of a report stating that a specific percentage of the interface exchanges have been successful. If anecdotal evidence gathered from discussions with personnel from both groups along with the judgment of the evaluator indicates that the interface is functioning well, then the Quality indicator "____% of interface exchanges are handled according to requirements" may be considered to be met.

Improvement – TBD

Caution for evaluators: during an evaluation, you may find additional groups to talk with, and, in talking with those groups, find even more groups. Be careful not to unnecessarily extend the evaluation into peripheral groups whose participation in incident management is marginal, at best.

Incident Management Capability Metrics				
0. General Metrics				
0.1 Organizational Interfaces				
0.1.1	**Have well-defined, formal interfaces for conducting agency incident management activities been established and maintained?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ Formal interfaces for conducting incident management activities in the organization have been defined.	Y ❑	N ❑

Prerequisites

- ❑ There is (or should be) an interface between the groups [R]

Controls

- ❑ Personnel in both groups are appropriately trained on the requirements, procedures, and relevant technology for implementing this interface [R]
- ❑ Both parties define and maintain a documented interface (e.g., email, MOU, MOA, LOA, SLA, procedure, or formal contract) that includes
  - Roles and responsibilities [R]
  - Requirements for exchange of information or data [R]
  - Required timeframes/criteria, as applicable, for the exchange of information or data [R]
  - Verification of receipt, as appropriate, for exchange of information or data [R]
  - Requirements for making any decisions (criteria, timeframe, content, scope) affecting either party [R]
  - Process and POCs for resolution of conflicts or issues
  - Process for review and modification of interface agreement

Activity

- ❑ Both parties use this interface to perform their work [R]
- ❑ Mock exercises are held to test the effectiveness of the interface under different conditions

Supporting Mechanisms

- ❑ Up-to-date contact information (e.g., phone, email) [R]
- ❑ Alternate forms of communication for POCs (and alternates) for both parties [R]

Artifacts

- ❑ Samples of logs or reports produced by these interactions
- ❑ Documentation of the interface (e.g., email, MOU, MOA, LOA, SLA, procedure, or formal contract, work process flows, organization charts) [R]
- ❑ Samples of information or data exchanged between groups

Quality

- ❑ Personnel in both groups are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ There is a process and criteria for periodically evaluating and improving the quality of performance and artifacts associated with this/these interfaces [R]

Regulatory References:

Guidance References:

Internal Organization References:

PROTECT: SECTION 1 OF INCIDENT MANAGEMENT CAPABILITY METRICS

The mission of the Protect process is to adequately protect and secure critical organization data and assets including the computing infrastructure of the groups performing incident management functions and their constituency, in response to current risk, threats, and attacks while handling information in a timely, secure fashion.

The Protect process focuses on efforts to

- evaluate the security posture of the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations after setting appropriate management approvals
- implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure
- pass off to the Detect process any information about ongoing events or incidents, discovered vulnerabilities, or other security-related events
- implement infrastructure protection improvements resulting from incident postmortem reviews or other process improvement mechanisms

An incident management capability has a role in the protection of an organization's networks by helping to prevent incidents from occurring as well as detecting and containing those incidents that do occur. This can take the form of providing the protect functions directly, or by providing guidance, recommendations, and assistance to those who perform the protect functions. For instance, information can be provided to business owners of organization networks and systems about recommended security best practices, configuration guidelines, filtering policies, vulnerability patching and remediation strategies, general security awareness training, and other activities. Information can also be provided on methods for containing or mitigating incidents by making changes within the infrastructure. Helping to fortify these systems and networks decreases the potential for successful attacks against the organization's infrastructure and helps contain and reduce any impact on organizational goals, objectives, and operations. There should be established interfaces with other parts of the organization (internal and external[5]) that are providing security operations management activities that are involved in the Protect process. Information on configuration management, patch management, and change management activities should be shared across this interface.

There are a variety of standards and best practices that organizations can use to provide guidance for proactively securing and hardening their infrastructure, for example[6]:

- ISO 17799 (ISO/IEC 17799:2005) [ISO 2005a]
- ISO 27001 (ISO/IEC 27001:2005) [ISO 2005b]
- Control Objectives for Information and related Technology (COBIT) [ITGI 2006]

[5] An external interface may be with managed security service provider, for example.

[6] See the Bibliography for complete reference information.

- Federal Financial Institutions Examination Council (FFIEC) Handbooks [FFIEC 2002]
- International Information Systems Security Certification Consortium (ISC)[2] Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) [ISC2 2005]
- Information Security Forum Best Practices [ISF 2005]
- Information Technology Governance Institute (ITGI) sources [ITGI 2006]
- IT Infrastructure Library (ITIL) [OGC 2006]
- National Institute of Standards and Technology (NIST) FIPS PUB 199, FIPS PUB 200, and Special Publications 800 series [NIST 2004, 2006, 2007]
- SEI body of work including the Capability Maturity Model Integration (CMMI), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and Security Knowledge in Practice (SKiP) [SEI 2002, 2003, 2005,]

Within the Protect category, the sub-groupings include

- **Risk Assessment Support**[7] – for measuring the computer security posture of information systems and computer networks. This category also includes vulnerability scanning and assessment functions.
- **Malware Protection Support** – incident management personnel play a vital role in the protection of the constituency's networks, alerting system and network operations personnel to new malicious code (e.g., viruses, worms, spyware) and assisting when an incident occurs.
- **Computer Network Defense Operational Exercises** – mock exercises that test the response plans and reactions of incident management personnel and the organization to various incident and vulnerability scenarios.
- **Constituent Protection Support and Training** – incident management personnel must be knowledgeable about the organization's network configurations in order to assist with "hardening" systems and correcting vulnerabilities identified in network configurations. The intent is that incident management personnel will participate in efforts to transition computer security knowledge and awareness to the community it serves.
- **Information Assurance/Vulnerability Management** – a positive control system that participates in identifying new system vulnerabilities and notifies the appropriate parts of the organization to enable the application of effective countermeasures. Incident management personnel monitor constituent compliance with vulnerability recommendations and prevention strategies, as well as provide technical support as required.

[7] Examples are assessment tools such as the National Institute of Standards and Technology (NIST) Computer Security Expert Assist Team (CSEAT) [NIST 2005] and the Software Engineering Institute (SEI) OCTAVE Method [SEI 2003].

1.1 Protect

1.1 Risk Assessment

1.1.1 Are Risk Assessments (RAs) performed on constituent systems?

Response to this question ascertains whether risk assessments (RAs) are performed on the organization's or constituents' systems (function 4.6.4 addresses risk assessments on incident management systems). Risk assessments should be used to identify weaknesses and problems in the infrastructure and organizational security practices before they can be exploited. This allows problem areas to be mitigated proactively, increasing the overall security of the organization. Incident management personnel may or may not be involved in performing the risk assessments, but they should have access to the results, even if the risk assessments are conducted by third parties.

Not applicable – Note that even if incident management personnel never actually provide any assistance, they should have access to the lessons learned from risk assessments as a means of staying informed about the current security posture of the organization and to improve the incident management capability. This function may be conducted via third-party contracting, and that contractor may or may not be included in this evaluation.

Impact statement – A thorough risk assessment provides a valuable means of proactively identifying and repairing risks in technology, process, and people, before such weaknesses can be exploited.

Scoring and interpretation guidance – The question is answered satisfactorily when risk assessments are conducted on constituent systems. This is a Priority I function and the question can only have a Yes or No answer. Specifically, the scoring guidance is as follows:

- A [Yes] answer for this question can be achieved if all required items are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- formalized procedures, guidelines, and training including how to perform risk assessments; how to determine if the assessment will interfere with other incident management operations (situational awareness); and how to mitigate risks that are found
- quality assurance checks on the type of risk assessment method and the information produced to ensure that it is complete, timely, accurate, clear, up to date, useful, and meets any organization, institutional or legal compliance guidelines
- training for personnel on the types of RAs available; sources that provide this service; how to choose which type of RA is most appropriate; or specific RA methods. Incident management personnel providing this service should be knowledgeable in the appropriate RA methods.

Incident Management Capability Metrics				
1. Protect				
1.1 Risk Assessment				
1.1.1	**Are Risk Assessments (RAs) performed on constituent systems?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Risk assessments are periodically performed and the results are used to improve the security posture of the organization.	Y ❑	N ❑

Prerequisites

- ❑ Management has given approval for RAs to be conducted on the constituent systems and networks [R]
- ❑ Incident management personnel have access to the results of RAs if they do not actually perform them [R]

Controls

- ❑ Documented procedures exist for conducting the risk assessment (e.g., COBIT, OCTAVE®) or for contracting with a third party to conduct the risk assessment [R]
- ❑ Documented policies and procedures exist that describe the process by which the results of risk assessments are analyzed [R]
- ❑ Personnel are appropriately trained on the procedures, process, methods, and supporting technologies used to provide conduct or contract for RAs [R]
- ❑ Guidelines exist for requesting RA assistance from the incident management personnel

Activity

- ❑ Risk assessments are performed on constituent systems [R]
- ❑ Technical assistance is provided to constituent for performing RAs [R]
- ❑ Results of RAs are provided to the constituent [R]
- ❑ RA results are tracked and recorded [R]
- ❑ Results of RAs are provided to incident management personnel [R]
- ❑ A list of RA providers and the type of assessments they perform (e.g., COBIT, OCTAVE®) is collected, maintained, and updated if third-party providers are used to perform RAs

Supporting Mechanisms

- ❑ Risk assessment tools and methods [R]
- ❑ RA results tracking and reporting tools and methods [R]
- ❑ Mechanisms for requesting assistance
- ❑ Mechanisms for providing assessment results and information to the requestor

Artifacts

- ❑ List of RA types and providers
- ❑ Copies of risk assessment results and improvement/mitigation actions [R]

Quality

- ❑ Personnel are aware, knowledgeable, and consistently follow the applicable procedures, processes, methodologies, and technologies for performing these activities [R]
- ❑ Risk analyses are archived in a secure and protected manner [R]
- ❑ Any communications of the risk analyses are done in a secure and protected manner [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(1) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."
Guidance References: None [indirect] NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems* [Swanson 2001] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec. 2.5 Incident Response Team Services [p 2-14, 2-15] "Vulnerability Assessment. An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. […] organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource."
Internal Organization References:

1.1.2 Are the constituents assisted with correcting problems identified by Risk Assessment (RA) activities?

This question focuses on the provision of technical recommendations, guidance, and support to the constituency to help with correcting security problems and vulnerabilities that have been identified in a risk assessment. Depending on the level and set of incident management services provided, the assistance given could take the form of hands-on configuration, where incident management personnel make the corrections or work with the appropriate system and network owner to make the changes, or the assistance could consist of offering technical remediation strategies and advice.

Not applicable – If another part of the organization handles the performance of risk assessments and actual mitigation, incident management personnel may only have access to the results for their information. The part of the organization that conducts risk assessments and assists with mitigation should be included in the evaluation.

Impact statement – Risk assessments without follow-on mitigation actions are a waste of resources.

Scoring and interpretation guidance – The function is satisfactorily performed when incident management personnel provide technical recommendations, strategies, and plans or actions to correct security problems and vulnerabilities in the constituent infrastructure that were identified by performing a risk assessment.

A [Yes] answer for this question can be achieved if all required [R] indicators are met.

The partial [P] grade for this metric can be achieved if

- the organization is in the process of developing such a capability or service OR
- analysis results are occasionally used to improve the security posture of constituent infrastructure network and systems OR
- the organization has informal procedures for completing this task AND
- personnel understand and follow the informal procedures consistently

Improvement – Improvement can be made by instituting quality assurance testing, ensuring all procedures are documented and tested, and by making sure all personnel are trained in the procedures and have a background in risk remediation techniques. Personnel will also require training for any other tasks that they may need to perform, such as vulnerability patching, security awareness training, or network defense configuration, as part of the remediation. Greater efficiency can also be achieved by maintaining and updating a prioritized list of criteria for how vulnerabilities might affect the infrastructure. This list can be used to determine which vulnerabilities must be addressed first. Further improvements can be made by using automated tools such as patch or configuration management systems. Any changes should be tracked and recorded and follow organization change management processes.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>1.1.2</td><td colspan="4">Are the constituents assisted with correcting problems identified by Risk Assessment (RA) activities?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed ❑</td><td rowspan="2">Not applicable ❑</td><td>Yes</td><td>▪ Detailed technical remediation support or assistance is provided to constituents for correcting problems identified by RA activities.</td><td rowspan="2">Y ❑</td><td rowspan="2">P ❑</td><td rowspan="2">N ❑</td></tr>
<tr><td>Partial</td><td>▪ Remediation capabilities are being developed.</td></tr>
<tr><td colspan="7">Prerequisites
❑ The RA results are accessible [R]
❑ Criteria for prioritizing risks based on business impacts exist [R]
Controls
❑ Documented policies and procedures for assisting constituents in applying remediation strategies for identified vulnerabilities exist [R]
❑ Procedures for documenting and archiving the remediation actions that are taken exist
❑ Personnel are appropriately trained about the policies and procedures for providing assistance to constituents [R]
❑ Personnel are appropriately trained on countermeasures and remediation strategies for risks [R]
Activity
❑ The results of the RAs are used to determine potential impacts and to make improvements to constituent infrastructure for prevention of computer security incidents [R]
❑ Recommendations for mitigating risks or security issues identified in RAs are provided [R]
❑ Remediation actions are performed for the identified risks or issues
Supporting Mechanisms
❑ Risk analysis and management tools
❑ Configuration and patch management systems
❑ Change management systems
Artifacts
❑ Copies of risk assessment results and corresponding improvement or mitigation actions [R]
❑ Copies of recommendations and remediation strategies provided to constituents for fixing identified risks in their infrastructure [R]
❑ Copies of follow-up reports showing that the problems were corrected
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedure, processes, and technologies for performing this task [R]
❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
❑ Risks and identified problems are successfully remediated or corrected __% of the time</td></tr>
<tr><td colspan="7">Regulatory References:
FISMA Sec 3544(b)(6) [OLRC 2003]
3544 “(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
‘‘(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency”
OMB Cir A-130 App III Sec A.5.a.
“Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.”</td></tr>
</table>

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec. 2.5 Incident Response Team Services [p 2-14, 2-15] "Vulnerability Assessment. An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. […] organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource."
Internal Organization References:

1.1.3 Is proactive vulnerability scanning (VS) performed on constituent networks and systems?

This question focuses on whether there is a defined process for performing vulnerability scanning (VS) and network monitoring on the enterprise infrastructure to ensure that vulnerabilities and anomalous behavior are identified and addressed in a timely manner to prevent or minimize damage to the organization. Depending on the range and level of incident management services provided and the expertise of incident management personnel, vulnerability scanning tasks can take many forms. Tasks can range from the simple provision of information on implementing vulnerability scanning methodologies and tools to actual performance of vulnerability scanning and analysis for the constituents. Constituents should be encouraged to proactively look for threats to their infrastructure to protect it from known attacks and vulnerabilities. This allows problem areas to be mitigated in a proactive manner, increasing the overall security of the organization.

As part of this process there should be guidelines for requesting assistance. Mechanisms such as templates or web forms for requesting scanning or other assistance may be made available. Assistance can be given via written or verbal recommendations, meetings, training sessions, or actual conducting of the scanning.

Not applicable – Note that even if incident management personnel never provide any assistance, they should have access to the lessons learned from vulnerability scans to improve the incident management capability.

Impact statement – TBD

Scoring and interpretation guidance – The function is satisfactorily performed when vulnerability scanning and analysis is performed. This is a Priority I function and the question can only have a Yes or No answer. Specifically, the scoring guidance is as follows:

- The [Yes] grade for this metric can be achieved only if all required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- formalized procedures, guidelines, and training, including how to provide notification, how to determine if the scanning will interfere with other incident management operations (situational awareness), and how to perform the vulnerability scanning methodology
- quality assurance checks on the information provided to ensure that it is complete, timely, accurate, clear and understandable, up to date, and useful, and meets any organization, institutional or legal compliance guidelines
- training for personnel on the methodologies and tools for vulnerability scanning. Personnel providing this assistance should be knowledgeable in methods to ensure they provide useful information to the requestor by making certain all relevant systems and networks are reviewed.
- automated tools for performing vulnerability scanning and tracking, including a vulnerability database that allows tracking of vulnerabilities by organizational or constituent unit, along with the ability to track vulnerability remediation

Incident Management Capability Metrics				
1.1.3	**Is proactive vulnerability scanning (VS) performed on constituent networks and systems?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Proactive vulnerability scanning (VS) is performed on constituent networks and systems.	Y ❑	N ❑

Prerequisites

- ❑ There is written permission from constituent management (or other documentation) to use VS tools [R]

Controls

- ❑ Documented policies and procedures exist
  - that describe the process and method by which permission for VS on constituent systems is obtained and assistance is provided to the constituents [R]
  - for performing the VS if they conduct this activity [R]
  - for analyzing data gathered from VS [R]
- ❑ Personnel are appropriately trained on the procedures, process, methods, and supporting technologies used to conduct VS and perform corresponding analysis [R]
- ❑ There is documentation that describes the VS tools and their potential impacts on constituent systems

Activity

- ❑ Proactive vulnerability scans are run on constituent networks and systems [R]
- ❑ VS tools are tested and evaluated prior to use on constituent systems [R]
- ❑ VS results are analyzed, recorded, and tracked [R]
- ❑ Constituents are alerted to any vulnerabilities found in their systems [R]

Supporting Mechanisms

- ❑ Mechanisms for constituent to request assistance
- ❑ Mechanisms for providing information to the requestor
- ❑ Vulnerability scanning tools and methodologies [R]
- ❑ Vulnerability tracking and reporting tools and methodologies [R]

Artifacts

- ❑ Authorization to install tools and perform scans
- ❑ Examples of any constituent request forms or written requests for assistance
- ❑ Copies of VS results and analysis [R]
- ❑ Copies of alerts or guidance to constituents for addressing problems identified by VS [R]

Quality

- ❑ Analyses are archived in a secure and protected manner [R]
- ❑ Any communications of the analyses are done in a secure manner [R]
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(5) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […] ''(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing— ''(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and ''(B) may include testing relied on in a evaluation under section 3545"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec. 2.5 Incident Response Team Services [p 2-14, 2-15] "Vulnerability Assessment. An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. These responsibilities can be extended so that the team performs auditing or penetration testing, perhaps visiting sites unannounced to perform on-the-spot assessments. Incident handlers are well suited to performing vulnerability assessments because they routinely see all kinds of incidents and have first-hand knowledge of vulnerabilities and how they are exploited. However, because the availability of incident handlers is unpredictable, organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource."
Internal Organization References:

1.1.4 Is the constituent assisted with correcting problems identified by vulnerability scanning (VS) activities?

This question focuses on the provision of technical recommendations, guidance, and support to the constituency to help with correcting security problems and vulnerabilities that have been identified via proactive vulnerability scanning. Depending on the level and set of incident management services provided, the assistance given could take the form of hands-on configuration, where incident management personnel make the corrections or work with the appropriate system and network owner to make the changes, or the assistance could simply be the provision of technical remediation strategies and advice.

Not applicable – TBD

Impact statement – TBD

Scoring and interpretation guidance – The function is satisfactorily performed when technical recommendations, strategies, plans, or actions are provided to correct security problems and vulnerabilities in the constituent infrastructure that were identified through proactive vulnerability scanning.

The [Yes] answer for this question can only be achieved if all required [R] indicators are met.

The [Partial] grade for this metric can be achieved if

- the organization is in the process of developing such a capability or service OR
- analysis results are occasionally used to improve the security posture of constituent infrastructure network and systems OR
- there are informal procedures for completing this task AND
- personnel understand and follow the informal procedures consistently

Improvement – Improvement can be gained by instituting quality assurance testing, ensuring all procedures are documented and up to date, making sure all personnel are trained in the procedures and have a background in vulnerability remediation techniques. Personnel will also need sufficient skills or training for any other tasks that they may need to perform, such as vulnerability patching, security awareness training, or network defense configuration, as part of the remediation.

Teams can also improve by maintaining and updating a prioritized list of criteria for how vulnerabilities might affect the infrastructure and using this list to determine which vulnerabilities must be addressed first. Further improvements can be achieved by using automated tools such as patch or configuration management systems. Any changes should be tracked and recorded and follow organization change management processes.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>1.1.4</td><td colspan="4">Is the constituent assisted with correcting problems identified by vulnerability scanning (VS) activities?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed ❑</td><td rowspan="2">Not applicable ❑</td><td>Yes</td><td>▪ Detailed technical remediation support or assistance is supplied to constituents for correcting problems identified by VS activities.</td><td rowspan="2">Y ❑</td><td rowspan="2">P ❑</td><td rowspan="2">N ❑</td></tr>
<tr><td>Partial</td><td>▪ Remediation capabilities are being developed or provided on an ad hoc basis.</td></tr>
<tr><td colspan="7">Prerequisites
❑ VS results are available [R]
❑ Criteria for prioritizing vulnerabilities based on business impacts exist
Controls
❑ Documented policies and procedures exist for
- assisting constituents in applying remediation strategies for identified vulnerabilities [R]
- documenting and archiving actions taken exist [R]
❑ Personnel are appropriately trained on
- the policies and procedures for providing assistance to constituents [R]
- countermeasures and remediation strategies for vulnerabilities [R]
Activity
❑ VS results are used to determine potential impacts and to recommend improvements to constituent infrastructure to prevent computer security incidents [R]
❑ Recommendations for correcting problems such as vulnerabilities or security issues identified in VS results are provided [R]
❑ Remediation of the identified problems is performed
❑ Follow-up actions are performed to ensure the problems are corrected and the actions are closed
Supporting Mechanisms
❑ Vulnerability tracking/handling mechanisms or systems [R]
❑ Configuration and patch management systems
❑ Change management systems
Artifacts
❑ Copies of recommendations and remediation strategies provided to constituents for fixing identified vulnerabilities in their infrastructure [R]
❑ Copies of follow-up reports showing that the problems were corrected
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedure, processes, and technologies for performing this task [R]
❑ There is a process and criteria (such as completeness, timeliness, accuracy, clarity, usefulness, and adherence to security best practices, institutional regulations, or legal rules and laws) for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
❑ Vulnerabilities and identified problems are successfully remediated or corrected __% of the time</td></tr>
</table>

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(6) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […] ‘‘(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency" OMB Cir A-130 App III Sec A.5.a. "Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above."
Guidance References: NIST 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-14, 2-15] "Vulnerability Assessment. An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. […] Incident handlers are well suited to performing vulnerability assessments because they routinely see all kinds of incidents and have first-hand knowledge of vulnerabilities and how they are exploited. However, because the availability of incident handlers is unpredictable, organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource."
Internal Organization References:

1.1.5 Is trend analysis supported and conducted?

This question focuses on whether the constituent organization takes a proactive, broad-based, big-picture view of the system and network incident and vulnerability information it is collecting in order to determine any trends in the types of attacks targeting the organization or changes in the types of malicious activity seen on the organization's infrastructure. This analysis can also show any patterns in the types of weaknesses being exploited in the organization, trends in the organization's security posture, or be helpful in identifying the root causes of security problems across the enterprise. These trends could show improvements or highlight repeating problem areas, for example

- any increase or decrease in the number of vulnerabilities and incidents
- any change in the types of vulnerabilities and incidents being reported
- recurring vulnerabilities and incidents
- changes in the scope of incident impact
- targeted areas of the organization vs. the entire enterprise

Not applicable – TBD

Impact statement – TBD

Scoring and interpretation guidance – The question is satisfied when personnel, with approval from management, follow defined procedures to perform this analysis using automated tools and incorporating all available data to help improve the security of the constituent systems. It is partially satisfied if the analysis is done manually or is not inclusive of all data or if only informal procedures are available. Specifically, the scoring guidance is as follows:

- The [Yes] grade for this question can be achieved if all the required indicators [R] are met.
- The [Partial] grade for this question can be achieved if
  - manual correlation is performed OR
  - there are informal procedures for completing this task AND/OR
  - trend analysis is performed using the output of some scanning or monitoring tools AND
  - performance analysis reports are provided to constituents AND
  - personnel understand and follow the informal procedures consistently AND
  - analysis results are occasionally used to improve the infrastructure or alter tool acquisition

Improvement – Improvement can be gained by

- ensuring tested, automated tools are set up to support collection of data for trend analysis in a consistent fashion
- ensuring all appropriate data from vulnerability scans, risk assessments, network monitoring, and other similar activities are incorporated into the trend analysis
- documenting all policies and procedures
- providing training to personnel on the best methods for performing trend analysis

- keeping an up-to-date list of vulnerabilities and problems discovered through trend analysis in a searchable database that can be used in identifying remediation actions or in future correlation and analyses

Incident Management Capability Metrics						
1.1.5	**Is trend analysis supported and conducted?**			**Priority III**		
Not observed ❑	Not applicable ❑	Yes	▪ Trend analysis is conducted using the results from other proactive analyses such as risk analysis, vulnerability scanning, and system monitoring activities.	Y ❑	P ❑	N ❑
		Partial	▪ Manual correlation is performed OR ▪ Trend analysis is conducted informally or occasionally.			

Prerequisites

- ❑ Proactive risk analysis, vulnerability scanning, and network and system monitoring activities are performed [R]
- ❑ Proactive analysis and monitoring data are accessible to support trend analysis [R]

Controls

- ❑ Criteria for what should be captured and included in the trend analysis exist [R]
- ❑ Documented policies and procedures exist detailing how to perform trend analysis, disseminate information, and archive actions taken [R]
- ❑ Personnel are appropriately trained about the policies, procedures, methods, and tools for collecting information and data and then performing trend analysis [R]

Activity

- ❑ Trend analysis is performed using the results from other proactive risk analysis, vulnerability scanning, and network and system monitoring activities [R]
- ❑ Trend analysis results are provided to designated individuals [R]
- ❑ Results of trend analysis are used to identify needed improvements to the security posture of constituent systems

Supporting Mechanisms

- ❑ Vulnerability tracking database
- ❑ Outputs from vulnerability scanning, network monitoring and other data collection and analysis tools [R]
- ❑ Trend analysis methods, tools, and programs [R]
- ❑ Automated trend analysis tools

Artifacts

- ❑ Copies of trend analysis reports [R]
- ❑ Documentation of actions that were taken [R]

Quality

- ❑ Vulnerability tracking database is kept up to date
- ❑ Personnel are aware of, knowledgeable of, and consistently perform the procedures for this activity [R]
- ❑ There is a process and criteria (such as completeness, timeliness, accuracy, clarity, and usefulness of the trend analysis) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: None [indirect] FISMA Sec 3544(b)(3) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-15] "Technology Watch. A team can perform a technology watch function, which means that it looks for new trends in information security threats. […] The team should then make recommendations for improving security controls based on the trends that they identify. A team that performs a technology watch function should also be better prepared to handle new types of incidents."
Internal Organization References:

1.2 Malware Protection

1.2.1 Is there an institutionalized Malware/Anti-Virus (AV) Program?

This question focuses on the ability to assist constituents with malware detection, analysis, and response. Malware can include viruses, worms, Trojan horse programs, spyware, rootkits, and other attack vectors. A malware capability includes

- installing and maintaining anti-virus and anti-spyware software tools across the enterprise
- public and private monitoring of anti-malware sites and organizations
- alerting constituents to the potential or current malware threat and remediation guidance
- keeping up to date on malware through research, training, mentoring, and other professional development efforts
- coordinating with other internal and external parties such as vendors, coordinating CSIRTs, ISPs, anti-virus groups, law enforcement, and other security experts to contain and eliminate threats and malicious activity
- properly reporting malicious activity to approved collaborators, partners, or upper management

Organizational collaboration and coordination of malware support will require defined processes, roles, and responsibilities internally and externally. Alerting and reporting of potential or real-time malicious activity should be done through multiple communication channels, such as email, FAX, phone, web sites, publications such as advisories or bulletins, and other broadcast mechanisms. If personnel are responsible for providing 24/7 support, they should be reachable via pager, cell phone, or email at all times. POC lists for malware experts, vendors, and other security organizations should be available.

Not applicable – Note that even if incident management personnel do not perform this function, they should have access to the results of the malware program to improve the incident management capability.

Impact statement – TBD

Scoring and interpretation guidance – The goal of satisfying this question is to show that incident management personnel are able to consistently, accurately, and reliably assess the risk or threat of a confirmed malware incident to the constituents' networks or systems and respond accordingly. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer to this question [Yes] can be achieved if all required [R] indicators are met.
- Any other combination of indicators is insufficient and results in a [No].

The prerequisite states there must be current documentation on critical constituent systems and the assets on those systems. Without this information, risk or threat can only be evaluated in an abstract, theoretical sense.

Improvement – Improvements can be implemented by

- implementing an enterprise-wide program for automatic updates

- considering the use of multiple A/V products from different vendors for more robust coverage of anti-virus signatures
- instituting a 24x7x365 malware capability
- monitoring anti-virus web and alert sites and mailing lists on a daily basis
- having defined document types and corresponding templates for disseminating information
- improving malware analysis techniques, building a test environment or lab facility, adding automated tools for collecting information on malware
- developing technical relationships with trusted experts (e.g., A/V vendors, CERT/CC)
- keeping POC lists up to date, with at least weekly or monthly review/refresh rates
- coordinating reports on a consistent and timely basis with appropriate contacts
- training end-user staff to recognize various types of malware and in timely reporting of malware activities
- training end-user staff in how to prevent malware attacks by following best practices in secure use of their systems

Incident Management Capability Metrics				
1.2 Malware Protection				
1.2.1	**Is there an institutionalized Malware/Anti-Virus (AV) Program?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is an institutionalized Malware/Anti-Virus Program that includes installed AV software and automated updates, documented guidance for preventing, detecting, reporting, and handling malware activity.	Y ❑	N ❑

Prerequisites

- ❑ List of constituent critical assets and data [R]

Controls

- ❑ Documented policies and procedures exist that describe the process and method by which this program is provided to the constituents, including notifications, alerts, and remediation assistance [R]
- ❑ Documented policies and procedures exist that define reporting requirements when malware is discovered including working with vendors or other external entities
- ❑ Personnel are appropriately trained on the procedures, process and supporting technologies used to identify, analyze, and remediate malware [R]

Activity

- ❑ A current list of POCs for notifications and alerts is maintained
- ❑ Sources for information on emerging malware (e.g., FIRST, CERT/CC, vendor anti-virus sites, and other similar organizations) are reviewed
- ❑ The impacts of malware on constituent systems are analyzed
- ❑ Constituents are alerted to emerging or current malware threats [R]
- ❑ Remediation, response, and recovery solutions to malware occurrences and threats are provided [R]
- ❑ Documented anti-malware installation & update procedures are provided to appropriate personnel
- ❑ Constituents are advised of sources for anti-malware signature updates
- ❑ Malware outbreaks and remediation are tracked and recorded [R]
- ❑ US-CERT and other anti-malware organizations are coordinated with on the development of countermeasures

Supporting Mechanisms

- ❑ Available, approved anti-malware software is used in accordance with organizational requirements [R]
- ❑ Automatic update mechanisms for patch and remediation [R]
- ❑ Web site for posting anti-malware files for constituents to download
- ❑ Alerting and dissemination mechanisms such as email lists or web sites [R]

Artifacts

- ❑ Up-to-date POC list with individual names and phone numbers
- ❑ Example of virus infection reports and statistics [R]
- ❑ Recent email or web malware warnings and advisories [R]
- ❑ Recent information from vendors on products and/or services on file

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently perform the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ❑ Malware is reported to appropriate parties within required timeframe of discovery
- ❑ Malware incidents are handled in a timely manner

Incident Management Capability Metrics
Regulatory References: None [indirect] FISMA Sec 3544(b)(3) and (7) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […] ''(7) procedures for detecting, reporting, and responding to security incidents […]"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 5 Handling Malicious Code Incidents (includes Sec 5.1 Incident Definitions and Examples, Sec 5.2 Preparation, Sec 5.3 Detection and Analysis, Sec 5.4 Containment, Eradication, and Recovery, Sec 5.5 Checklist for Handling Malicious Code Incidents, and Sec 5.6 Recommendations)
Internal Organization References:

1.3 Computer Network Defense Operational Exercises

1.3.1 Are operational exercises conducted to assess the security posture of the organization?

This question focuses on how operational exercises are conducted. These exercises may involve Red Teams, mock or test incident exercises, penetration testing, table top or other comparable exercises. They may be internal to the organization or part of broader, inter-organization exercises (although broader multi-organization exercises should NOT be the only form of operational exercise conducted). The type of operational exercises that are approved and performed may be designated by organization or determined by other requirements. This question covers multiple types of activities that might be performed as part of this function, such as

- maintaining a vetted list of POCs as sources of operational exercises
- helping constituents choose or find a source for operational exercises or alternatives
- actually performing, conducting, or coordinating the operational exercise

The intent is to ensure that operational exercises of some kind are conducted and that they are conducted by reliable, capable, and vetted sources.

Not applicable – TBD

Impact statement – Operational exercises test the incident management capability and the security of an organization and its corresponding infrastructure, providing lessons learned that will help improve the security posture of the organization.

Scoring and interpretation guidance – The function is satisfactorily answered when there are documented policies, procedures, and guidance for performance and notification of operational exercises. The function is partially satisfied if exercises are occasionally performed in an ad hoc, undocumented way. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - operational exercises are performed or supported in a limited or ad hoc manner AND
  - operational exercises analysis and lessons learned are provided to appropriate management and technical personnel AND
  - personnel understand and follow the informal procedures consistently

Improvement – Improvement can be achieved by

- implementing formalized procedures, guidelines, and training, including how to provide notification, how to determine if the exercise will interfere with other incident management operations (situational awareness), and how to follow the methodology
- keeping all POC lists and source information up to date
- implementing a plan for quarterly testing that uses various combinations of techniques or approaches (such as penetration testing in combination with mock exercise, etc.)

Incident Management Capability Metrics						
1.3 Computer Network Defense Operational Exercises						
1.3.1	**Are operational exercises conducted to assess the security posture of the organization?**			**Priority III**		
Not observed ❑	Not applicable ❑	Yes	▪ Operational exercises are conducted periodically or upon request.	Y ❑	P ❑	N ❑
		Partial	▪ There are limited, ad hoc operational exercises.			

Prerequisites

- ❑ Organization management has given approval and guidance for performing operational exercises on the constituent systems and networks [R]

Controls

- ❑ Documented policies requiring periodic testing or audit of organization security exist
- ❑ Policies and procedures exist that outline roles, responsibilities, scope, appropriate tools and notification requirements for operational exercises [R]
- ❑ Documented guidance for performing the operational exercises exists [R]
- ❑ Documented guidance for validating current policies and procedures during operational exercises exists.
- ❑ Personnel are appropriately trained on the procedures, process and supporting technologies used to conduct operational exercises [R]

Activity

- ❑ A list of types and sources (e.g., other departments or organizations) for operational exercises is maintained
- ❑ Personnel help the constituent with identifying the need for operational exercises, the most appropriate type of exercise, and sources
- ❑ Personnel perform or support operational exercises [R]
- ❑ Appropriate personnel are notified of operational exercises per guidance
- ❑ Current policies and procedures are validated during operational exercises

Supporting Mechanisms

- ❑ Exercise plans
- ❑ Software for penetration testing
- ❑ Incident reporting systems or mechanisms

Artifacts

- ❑ Exercise materials or scenarios
- ❑ Recommendations on types and sources of exercises provided to constituents
- ❑ Results and lessons learned from exercises [R]
- ❑ POC list with appropriate organizations and trusted agents to contact
- ❑ Descriptions of potential impacts on constituent systems from operational exercises

Quality

- ❑ Operational exercises are conducted more often than annually
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ Information on operational exercises is up to date, accurate, and relevant
- ❑ The results of operational exercises are used to improve the security posture of the organization [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(5) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing— ''(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and ''(B) may include testing relied on in a evaluation under section 3545,
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.4.3 Incident Response Personnel [p 2-12] "Develop incident handling scenarios and have the team members discuss how they would handle them. Appendix B contains a set of scenarios and a list of questions to be used during scenario discussions" [p 2-13] "Conduct simulated incident handling exercise for the team. Exercises are particularly important because they not only improve the performance of the incident handlers, but also identify issues with policies and procedures, and with communication." and App B Incident Handling Scenarios [p B-1] "Organizations are strongly encouraged to adapt these questions and scenarios for use in their own incident response exercises." [indirect] Sec 2.3.1 Policy and Procedure Elements [p 2-4] "SOPs should be tested to validate their accuracy and usefulness […]"
Internal Organization References:

1.3.2 Are lessons learned from operational exercises incorporated into the constituents' network defenses?

This function looks at how technical recommendations, guidance, and support are provided to the constituents to help them incorporate lessons learned from operational exercises. Depending on the incident management services provided, the assistance given could take the form of hands-on assistance, where incident management personnel make the corrections or work with the system and network owner to make the changes, or the assistance could be the provision of technical remediation strategies, training, advice, and guidance.

Not applicable – TBD

Impact statement – TBD

Scoring and interpretation guidance – The function is satisfactorily performed when the constituent is provided with the assistance needed to incorporate lessons learned from operational exercises. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met:
- The [Partial] grade for this question can be achieved if
  - there are informal procedures for completing this task AND
  - personnel understand and follow the informal procedures consistently AND
  - personnel assists the constituents in incorporating the lessons learned on an occasional basis OR
  - personnel send feedback on lessons learned to the appropriate contacts

Improvement – Improvements can be gained by instituting a quality assurance review of the assistance provided, by verifying that lessons learned are incorporated, and by validating that improvements are made and were beneficial.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>1.3.2</td><td colspan="4">Are lessons learned from operational exercises incorporated into the constituents' network defenses?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ The results of operational exercises are analyzed and the constituent is assisted with incorporating lessons learned to improve their network defenses.</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ Operational exercise results are informally or occasionally analyzed and constituents are occasionally assisted with incorporating lessons learned to improve their network defenses.</td></tr>
<tr><td colspan="7">Prerequisites
❑ There are operational exercise lessons learned results that can be accessed [R]
❑ The constituents have designated who is to implement appropriate lessons learned [R]
Controls
❑ Documented policies and procedures for assisting constituents in applying lessons learned exist [R]
❑ Personnel are appropriately trained about the policies and procedures for providing assistance to constituents [R]
❑ Personnel are appropriately trained on best practices, methodologies, and remediation strategies for hardening network and system defenses and mitigating organizational security weaknesses [R]
Activity
❑ Analysis of results of operational exercises and documentation of recommendations is performed [R]
❑ Recommendations are provided for correcting problems such as vulnerabilities or security issues identified in operational exercises [R]
❑ Remediation is performed
Supporting Mechanisms
❑ Vulnerability tracking/handling systems
❑ Configuration and patch management systems
❑ Change management systems
❑ Tools for monitoring and hardening systems and networks
Artifacts
❑ Copies of analysis results from the operational exercises
❑ Copies of recommendations and remediation strategies provided to constituents for incorporating lessons learned into their infrastructure [R]
❑ Copies of follow-up reports showing that lessons learned were incorporated
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedure, processes, and technologies for performing this task [R]
❑ Applicable lessons learned are successfully incorporated __% of the time
❑ There is a process and criteria (such as completeness, timeliness, accuracy, clarity, usefulness, and adherence to security best practices, institutional regulations, and laws) for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
<tr><td colspan="7">Regulatory References:
FISMA Sec 3544(b)(6) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
''(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency"</td></tr>
</table>

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.4 Post-Incident Activity Sec 3.4.1 Lessons Learned [p 3-22 and 3-23] "Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major incident […] is extremely helpful in improving security measures and the incident handling process itself. […] Questions to be answered […] include— […] What corrective actions can prevent similar incidents in the future?" and Sec 3.4.2 Using Collected Incident Data [p. 3-23] "A study of incident characteristics may indicate systemic security weaknesses and threats […]. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls." [indirect] Sec 2.4.3 Incident Response Personnel [p 2-12] "Develop incident handling scenarios and have the team members discuss how they would handle them. Appendix B contains a set of scenarios and a list of questions to be used during scenario discussions" [p 2-13] "Conduct simulated incident handling exercise for the team. Exercises are particularly important because they not only improve the performance of the incident handlers, but also identify issues with policies and procedures, and with communication." and App B Incident Handling Scenarios [p B-1] "Organizations are strongly encouraged to adapt these questions and scenarios for use in their own incident response exercises."
Internal Organization References:

1.4 Constituent Protection Support and Training

1.4.1 Is there a list of which systems, data, and information are mission critical?

This function focuses on understanding the organization's critical systems and the data that must be protected. There should be current information about what is on an organization's networks and systems so as to best assess protection requirements and to ensure a timely and appropriate response. It should also ensure legal compliance with regulations or laws (e.g., to make sure information is released or accessed in an authorized fashion). When an event, incident, or vulnerability is reported, this information allows impacts to be assessed in light of the criticality of the data or system. If the location of critical data is not known then notification to end users and other relevant parties, according to compliance laws, may be delayed or not occur.

If possible, there should be up-to-date configuration information for all supported organization networks and systems. Configuration information can include

- a list of IP address ranges and responsible administrative personnel or ISOs
- the latest constituent network diagram(s)
- an up-to-date inventory of information systems, network components, application software, operating systems, and network services utilized by constituents
- a list of network access points and their operational importance

Not applicable – Not all incident management personnel, especially those in distributed control environments, will have direct access to such configuration information. In that case, they may need to establish a formal interface with the part of the organization that does have this information. This interface can also be used as a means of coordinating improvements to system and network configurations based on trend analysis, incident history, and incident management staff expertise. Where possible the organization can benefit by involving incident management personnel in the change management process to ensure knowledge about infrastructure changes is appropriately shared from a security perspective and also to allow incident management personnel to have security-related input in needed changes.

Impact statement – Knowing the critical systems, data, and information to be protected ensures that the personnel involved in incident management functions are focusing the right resources on protecting the right assets.

Scoring and interpretation guidance – The function is satisfactorily performed when there is consistent and up-to-date information or access to information on mission-critical systems, data, and information. This is a Priority I function and the question can only have a Yes or No answer. The scoring guidance is

- A [Yes] answer for this metric can be achieved if all required [R] items are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- a process to ensure that this information and POC for updating this information are kept up to date

- a process to ensure that incident management personnel are included in any change management system and change notices
- a process to ensure that incident management personnel have a way to provide input to the configurations and defense strategies for critical systems and data
- an automated system to record and track critical data and systems that can be integrated with any incident handling or tracking system

Incident Management Capability Metrics				
1.4 Constituent Protection Support and Training				
1.4.1	**Is there a list of which systems, data, and information are mission critical?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ Up-to-date, accurate, and complete information on the mission critical systems, data, and information is maintained.	Y ❑	N ❑

Prerequisites
- ❑ Criteria exist that defines what systems, data and information are mission critical [R]
- ❑ The organization has identified its mission critical systems, data, and information [R]

Controls
- ❑ Documented policies and procedures exist that describe the process and method by which the information is obtained, stored, and used [R]
- ❑ Documented procedure exists for contacting personnel responsible for critical systems, data, and information
- ❑ Personnel are appropriately trained on the policies, procedures, and technologies employed to obtain, store, and use this information [R]

Activity
- ❑ Personnel have access to an up-to-date and accurate list of mission critical systems, data, and information [R]
- ❑ This list of mission critical systems, data, and information is used to assess the impact and determine response strategies and priorities for computer security events, incidents, and weaknesses [R]

Supporting Mechanisms
- ❑ Database or other mechanism for tracking mission critical systems, data, and information
- ❑ Change and configuration management systems
- ❑ Incident handling and tracking system
- ❑ Vulnerability tracking, patch management systems

Artifacts
- ❑ Lists or database of critical systems, data, and information [R]
- ❑ POCs for critical systems, data, and information

Quality
- ❑ The list is sufficiently detailed to enable analysts to determine if an event or incident affects mission critical systems, data, or information [R]
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information [R]
- ❑ Information is archived in a secure and protected manner [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Incident Management Capability Metrics
1.4 Constituent Protection Support and Training
Guidance References: NIST 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.6 Incident Prioritization [p 3-14] "Criticality of the Affected Resources. Resources affected by an incident (e.g., firewalls, Web servers, Internet connectivity, user workstations, and applications) have different significance to the organization. The criticality of a resource is based primarily on its data or services, users, trust relationships and interdependencies with other resources, and visibility (e.g., a public Web server versus an internal department Web server). Many organizations have already determined resource criticality through their business continuity planning efforts or their Service Level Agreements (SLA), which state the maximum time for restoring each key resource. When possible, the incident response team should acquire and reuse existing valid data on resource criticality." [indirect] NIST SP 800-59 *Guideline for Identifying an Information System as a National Security System* [Barker 2003]
Internal Organization References:

1.4.2 Is guidance provided to constituents in best practices for protecting their systems and network?

This function focuses on whether there is a defined process and methodology to provide constituent guidance on best practices for protecting systems and networks. These best practices can include methods for hardening system and network components, configurations, or perimeter defenses (such as firewalls and routers). Guidance can be given via training, presentations, mentoring, advisories, or other written technical publications. Guidance can be general or focus on specific constituent network and system components.

If it is available, having access to constituent network diagrams, configurations, and critical systems and data can help determine the most appropriate guidance to provide. As part of this process there should be defined policies, procedures, and processes for developing, disseminating, and updating recommendations and guidance.

Not applicable – TBD

Impact statement – Guidance to constituents raises their awareness and provides recommendations for making improvements, allowing problem areas to be proactively mitigated, increasing the overall security of the constituent infrastructure, and thereby improving the security posture of the organization.

Scoring and interpretation guidance – The function is satisfactorily performed when current and appropriate guidance or best practices for securing systems and networks is provided in a written, consistent, timely fashion. The question is partially satisfied if the guidance is provided verbally or via informal mechanisms. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - the guidance is provided verbally OR
  - the guidance is provided infrequently or in an ad hoc manner AND
  - there are informal procedures for completing this task AND
  - personnel understand and follow the informal procedures consistently

Improvement – Improvement can be achieved by implementing

- formalized procedures, guidelines, and training, including how to develop guidance, how to disseminate guidance, how to create training and presentation materials, and how to provide training
- quality assurance checks on the information provided to ensure that it is complete, timely, accurate, clear and understandable, up-to-date, and useful, and meets any organization, institutional, or legal compliance guidelines
- training programs for personnel on the methods for securing and hardening systems and networks
- methods for updating guidance materials on a periodic basis

Incident Management Capability Metrics						
1.4.2	**Is guidance provided to constituents in best practices for protecting their systems and network?**			**Priority III**		
Not observed ❑	Not applicable ❑	Yes	▪ Guidance is provided in best practices through training, presentations, and technical publications on a regular basis.	Y ❑	P ❑	N ❑
		Partial	▪ Provided guidance is ad hoc or informal.			

Prerequisites

- ❑ Best practice information exists or can be accessed via publicly available resources [R]

Controls

- ❑ Documented procedures exist for providing and updating general best practice guidelines for protecting constituents systems and networks [R]
- ❑ Documented policies and procedures for disseminating best practice information exist [R]
- ❑ Personnel are appropriately trained on
  - best practices and strategies for protecting constituent systems and networks [R]
  - the procedures, process, and supporting technologies used to provide guidance on best practices [R]

Activity

- ❑ Guidance is provided to constituents on best practices for protecting constituent systems and networks [R]
- ❑ Training or presentations on best practices for protecting constituent systems and networks is provided
- ❑ Methods are recommended for hardening network and system configurations generally and for specific constituent infrastructure components such as firewalls, IDS, routers, desktops, and other infrastructure components

Supporting Mechanisms

- ❑ Instructional materials and guidance [R]
- ❑ Display and distance education equipment
- ❑ Web sites
- ❑ Publishing software

Artifacts

- ❑ Constituent network diagrams and configurations
- ❑ Copies of recommended general and specific best practice guidance given to constituents
- ❑ Training or presentation material
- ❑ Technical publications providing best practice guidelines

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Personnel are aware and knowledgeable about security best practices [R]
- ❑ Best practice information is up to date, current, and relevant to the constituents [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(3) and (4) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […] ''(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— ''(A) information security risks associated with their activities; and ''(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.1.2 Preventing Incidents [p 3-3] "Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices. Other documents already provide good advice on general security concepts and operating system and application-specific guidance." [footnote 36] http://csrc.nist.gov/publications/nistpubs/ provides links to the NIST Special Publications on computer security, which include documents on operating system and application security baselines.
Internal Organization References:

1.4.3 Are constituents provided with security education, training, and awareness (ETA)?

This function measures the process and methodology by which the organization's security education, training, and awareness programs for constituents are provided. This provision can take many forms including identification of training requirements and gaps for each constituent group, providing of input for a security curriculum, or development and delivery of security training, education, or awareness. Incident management personnel can help identify where constituents require more guidance to better conform to accepted security practices and organizational security policies.

Security awareness can be increased through articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organization systems. Topics covered can include

- security guidelines (such as creating good passwords, handling secure data, or avoiding identify theft)
- malicious code types, propagation, and remediation techniques
- installing and using anti-virus software, personnel firewalls, or spyware detectors
- incident reporting guidelines detailing what, how, and to whom to report suspicious or malicious behavior
- appropriate incident prevention and response methods
- other information necessary to protect, detect, report, and respond to computer security incidents

Not applicable – Many organizations have mandatory security awareness training requirements so it is unlikely that this function is Not Applicable. However, if security is an outsourced capability, then it is possible that defining security ETA requirements is not provided by incident management personnel and that this function is the responsibility (overall) of the organization and the external service provider.

Impact statement – Increasing the general security awareness of the constituents not only improves their understanding of security issues but also helps them perform their day-to-day operations securely. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses.

Scoring and interpretation guidance – The function is satisfactorily performed when security education, training, and awareness are provided on a regular basis via a documented curriculum. Materials are written, consistent, and up to date. The question is partially satisfied if the organization provides security education, training, and awareness assistance on an intermittent basis using an undocumented curriculum. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the guidance is provided verbally OR

- the guidance is provided infrequently or in an ad hoc manner AND
- there are informal procedures for completing this task AND
- personnel understand and follow the informal procedures consistently

Improvement – Improvement can be achieved by

- implementing a formalized process
- building in quality assurance checks to ensure materials are current, accurate, and up to date
- training ETA-development personnel on instructional design and curriculum issues and methodologies
- training ETA-development and delivery personnel on security awareness best practices

Incident Management Capability Metrics						
1.4.3	**Are constituents provided with security education, training, and awareness (ETA)?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ Security education, training, and awareness assistance is provided on a regular basis using a documented curriculum.	Y ❑	P ❑	N ❑
		Partial	▪ Some security education, training, and awareness assistance is provided on an intermittent basis using an undocumented curriculum.			

Prerequisites

- ❑ There is a group or person designated as having responsibility for security and awareness training for the constituents [R]

Controls

- ❑ Documented procedures exist for providing and updating general security awareness training and education content [R]
- ❑ Documented policies and procedures exist for providing input into constituent security training curriculum interface
- ❑ Personnel are appropriately trained on the procedures, process, and supporting technologies used to provide security education, training, and awareness assistance [R]
- ❑ Personnel are appropriately trained on security awareness program methods and best practices [R]

Activity

- ❑ Security education, training, and awareness assistance is provided [R]
- ❑ Constituents are assisted with identifying training requirements to strengthen areas of constituent weakness
- ❑ Training requirements are documented [R]
- ❑ ETA input for constituent security curriculum is provided by incident management personnel
- ❑ Periodic refresher training for security awareness is provided

Supporting Mechanisms

- ❑ Training and curriculum methods and equipment including classroom instruction, Computer-Based Training (CBT), web presentation, or distance learning
- ❑ Training and curriculum development systems and software

Artifacts

- ❑ Assessment reports of constituent ETA security program
- ❑ ETA requirements for constituents [R]
- ❑ Copies of training requirement recommendations made to constituents
- ❑ Training presentations and educational materials
- ❑ Constituent evaluations of training program(s)
- ❑ Security awareness posters, articles, or publications

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Personnel are aware of and knowledgeable about security awareness methodologies and practices [R]
- ❑ Provided ETA material and content are up to date, current, and relevant [R]
- ❑ There is a process and criteria (such as relevance, accuracy, completeness, and usefulness) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ❑ Security awareness training is mandatory for all employees [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(4) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— ''(A) information security risks associated with their activities; and ''(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks"
Guidance References: NIST 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-15] "Education and Awareness. Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops and seminars, Web sites, newsletters, posters, and even stickers on monitors."
Internal Organization References:

1.5 Information Assurance/Vulnerability Management

1.5.1 Is there a patch alert and management program?

This function focuses on the process for receiving alerts about patches, disseminating patch information to constituents, patching constituent systems, providing follow-up to ensure patches are correctly installed, and helping constituents to get extensions when patching cannot be implemented immediately. Patch information can be disseminated to constituents or the patches can be installed on constituent systems. There must be coordination with system and network administrators for systems that incident management personnel do not have control over, to ensure that those systems that need to be patched by the relevant system and network administrator are patched.

Incident management personnel should seek information about all patch notifications from as many sources as possible, including software and hardware vendors, other vulnerability analysis and reporting organizations, and other security experts. Tracking such notices, the impacts on constituent sites, and the actions taken in a database or tracking system can help keep a history of vulnerability actions for the organization and provide a source mechanism for trend analysis.

Patching may not be feasible for all systems, or may require significant testing, and some systems may require new system certifications if they are changed (patched). The organization needs to know which systems fall into these categories and ensure appropriate actions are taken to monitor those systems, conduct testing to prevent patches from affecting operational or production systems, and ensure appropriate actions are taken to mitigate security risks.

Not applicable – This function should never be Not Applicable.

Impact statement – Timely patch alerts and installation provide a method to protect systems from threats and to contain any malicious activity caused by exploitation of vulnerabilities. Patch management can help increase the security posture of the constituent organization by proactively protecting critical systems, networks, and data.

Scoring and interpretation guidance – This function is satisfactorily performed when notices of new patches are received, constituents are notified of available patches, the patches are installed (incident management personnel may provide assistance), and there are appropriate documented policies, procedures, and training for conducting these activities. This is a Priority I function and the question can only have a Yes or No answer. The scoring guidance is as follows:

- A [Yes] answer for this question can be achieved if all required [R] indicators are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- formalized procedures, guidelines, and training on providing assistance for patch management
- quality assurance checks on the information provided to ensure that it is complete, timely, accurate, clear and understandable, up to date, useful, and meets any organizational, institutional, or legal compliance guidelines
- training for CSIRT personnel on the patch mitigation and installation techniques and methodologies

- a process to keep all POC lists ands security mailing list subscriptions up to date
- automated tools for patch dissemination and installation

Incident Management Capability Metrics				
1.5 Information Assurance/Vulnerability Management				
1.5.1	**Is there a patch alert and management program?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Constituents are assisted in protecting their systems through alerts of new patches, guidance for installation of patches, monitoring of patch management activities, and performance of patch installation as appropriate.	Y ❑	N ❑

Prerequisites

- ❑ Current inventory or list of critical systems, data, and information is available [R]
- ❑ Current inventory of systems and applications that cannot be patched due to business, compliance, or other reasons is available [R]
- ❑ There are designated responsibilities for patch management [R]

Controls

- ❑ There are documented procedures for
  - patch installation, including notifying/coordinating with system owners/ administrators [R]
  - testing/verifying patches before installation [R]
  - disseminating patches and patch information [R]
  - monitoring patch implementation by constituents [R]
  - submitting and handling extension requests for constituency [R]
  - determining and implementing the actions needed to isolate an unpatched system [R]
- ❑ Personnel are appropriately trained on the procedures, processes, and supporting technologies
  - used to provide patch management assistance [R]
  - for patch installation, patch monitoring, and identifying remediation strategies for systems that cannot be patched [R]

Activity

- ❑ A current list is maintained of constituent POCs, with primaries and alternates to contact about alerts and patches, acknowledge receipt of patches, and track compliance and extension information [R]
- ❑ The organization receives vendor and other security group patch notifications (including the technical advisories) and actively manages patch information and alerts [R]
- ❑ Technical input is provided to constituents in the development of procedures for patch management/installation
- ❑ Constituents are alerted to potential threats and problems and the release of new patches
- ❑ Patches are distributed to constituents for installation or patches are directly installed on constituent systems [R]
- ❑ Patch implementation by the constituents is monitored and technical assistance is provided as required [R]
- ❑ Monitoring is coordinated with other responsible parties for systems not under direct incident management staff control
- ❑ Constituent patch procedures are reviewed for adequacy as needed
- ❑ Monitoring and coordination are adjusted to special circumstances/situations at constituent sites when patching must be delayed
- ❑ The constituency is assisted with extension requests, particularly with describing technical risks associated with noncompliance
- ❑ Processes are in place to monitor systems that cannot be patched

Supporting Mechanisms

- ❑ Automated tools for distributing and installing patches on constituent systems
- ❑ Mechanisms to notify incident management personnel and constituents of new patches [R]
- ❑ Archive where patch notifications (alerts, bulletins and advisories) are securely stored

Incident Management Capability Metrics
Artifacts ❑ Copies of patch alerts and notifications sent to constituents [R] ❑ Mail from vendors or others announcing patch availability [R] ❑ Copies of extension requests, if done ❑ Records of patches that have been installed [R] **Quality** ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this including patch installation, patch monitoring, and remediation strategies [R] ❑ Information on patches provided to constituents is up to date [R] ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R] ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
Regulatory References: None [indirect] FISMA 3544(b)(3) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]
Guidance References: NIST SP 800-40 *Procedures for Handling Security Patches* [Mell 2002] Sec 2 Creating and Implementing a Patching Process [p 5] "We recommend creating a "Patch and Vulnerability Group" (PVG)." and Sec 5 Patching Procedures NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-14] "**Advisory Distribution.** A team may issue advisories that describe new vulnerabilities in operating systems and applications and provide information on mitigating the vulnerabilities. Promptly releasing such information is a high priority because of the direct link between vulnerabilities and incidents. […] It is recommended that only a single team within the organization distribute computer security advisories, to avoid duplication of effort and the spread of conflicting information." [counter reference: CSIRT should *not* be given responsibility for patch management] NIST 800-61 Sec 2.5 Incident Response Team Services [p 2.15] "**Patch Management.** Giving the incident response team the responsibility for *patch management* (e.g., acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization) is generally not recommended. Patch management is a time-intensive, challenging task that cannot be delayed every time an incident needs to be handled. In fact, patch management services are often needed most when attempting to contain, eradicate, and recover from large-scale incidents. Effective communication channels between the patch management staff and the incident response team are likely to improve the success of a patch management program."
Internal Organization References:

DETECT: SECTION 2 OF INCIDENT MANAGEMENT CAPABILITY METRICS

In the Detect process, information about potential incidents, vulnerabilities, and other computer security or incident management information is gathered both proactively and reactively. In reactive detection, information is received from internal or external sources in the form of reports or notifications, as shown in the examples below:

- Those using the organization's computing resources may notice some unusual or malicious activity and report it to the appropriate contact. The reporting may involve submitting an incident reporting form or calling the appropriate POC, such as a help desk or a CSIRT hotline.
- Other computer security experts may send an alert or notification that must be assessed to see if there is a potential threat to the receiver's infrastructure. For example, some other external team might receive reports of a new worm propagating in its area, create an advisory or alert, and send it out to a subscriber mailing list. The organization's incident management personnel see this advisory or alert and evaluate whether it might have a similar effect in their constituency, then take action based upon their analysis.
- An external team might send a report to an organization alerting personnel to activity appearing to originate from within the organization. The organization then needs to review or evaluate its own systems to determine if there is a problem.

Proactive detection requires actions by the designated staff to identify suspicious activity. Personnel monitor a variety of data (such as host logs, firewall logs, and netflows) and use intrusion detection and prevention software to monitor network behavior, looking for indications of suspicious activity. The data are analyzed, and any unusual or suspicious event information is "triaged" to the appropriate individuals for handling.

Personnel performing proactive detect functions may be located in various parts of an organization such as IT, telecommunications group, security group, or a formal CSIRT. In some organizations, the IT or network operations staff perform this function and pass on any suspicious activity or relevant incident or vulnerability information to an established CSIRT. In such cases, it is important to have established procedures for passing on this information. Personnel performing the monitoring must have criteria to help them determine what type of alerts or suspicious activity should be escalated. Personnel who conduct proactive monitoring can include

- IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators)
- selected members of the CSIRT staff
- third parties (e.g., MSSPs, collaborators, ISPs, trusted subject matter experts)
- coordination center

Proactive detection also includes technology watch or public monitoring functions to evaluate current information about security topics that may affect the organization's computing infrastructure. Personnel review security resources to obtain information about new vulnerabilities, new attack types and threats, new recommendations and solutions for preventing incidents, or general political, social, or sector-related information that may have relevance to ongoing or potential malicious activity. Security resources would include, for example, security

mailing lists, web sites, articles, or news reports that are available publicly, or aggregated information from a commercial service.

The two subcategories in the Detect category are

1. **Network Security Monitoring** – Network monitoring is an important proactive function that allows an organization to detect suspicious activity across the enterprise. Such monitoring can provide early warnings about malicious threats or activity in the organization's infrastructures, allowing response actions to be initiated in a timely manner, containing the damage and impact that could have been done. Technologies involved in network monitoring and analysis can include intrusion detection systems (IDS), intrusion prevention systems (IPS), anomaly detection systems (ADS), anti-virus detection systems (AVS), netflow analysis tools, and network forensics analysis tools (NFAT). Incident management personnel might assist organizations with monitoring tool selection, configuration and installation, and analysis of output for detection of possible intrusions.
2. **Indicators, Warning, and Situational Awareness** – Organizations must understand the context within which network events and incidents occur. To do this they must keep up to date with new attack types, remediation strategies, detection strategies, best practice protection strategies, and security detection and response tools. However, to get a complete picture of the relationship of network and system traffic to current events, other political, social, economic, and financial activities must also be reviewed. This type of proactive monitoring of new and current developments is often called technology watch, public monitoring, and situational awareness. Such monitoring provides an overview of internet activity in the context of domestic and foreign developments. It can show connections between activity and attacks at different sites and help analysts better understand the scope and impact of malicious computer events and incidents.

2. Detect

2.1 Network Security Monitoring

2.1.1 Is there network monitoring of the constituent systems and networks?

Network monitoring is an important proactive (as well as reactive) function that allows an organization to detect suspicious activity across its enterprise. This can include

- monitoring constituents' systems
- helping or training constituents to monitor their own systems
- providing guidance and recommendations on tool selection, installation, and configuration, analysis and monitoring techniques and methodologies, or network monitoring strategies
- analyzing or monitoring output to detect possible intrusions
- notifying constituents of suspicious behavior

Technologies involved in network monitoring and analysis can include IDS, IPS, ADS, AVS, netflow analysis tools, NFAT, and other tools.

Not applicable – It is advisable for the organization to perform this function. Whoever performs this function, whether it be IT, local system administrators, or an established CSIRT, should be assessed relative to this function. In some organizations, monitoring might be completely outsourced to a third-party MSSP. The question would be applied to the MSSP if it is included in the evaluation. Note that in any case, the incident management capability needs an interface to whoever performs the monitoring to receive notifications of suspicious activity.

Impact statement – Monitoring can provide early warnings about malicious threats or activity in the organization's infrastructure, allowing a timely response and containing the potential damage. This improves the network defense posture of the organization and allows it to provide an agile response.

Scoring and interpretation guidance – This function is satisfactorily performed when the organization conducts network security monitoring and intrusion detection and prevention monitoring; disseminates the results of analysis; and forwards reports, alerts, and notifications to other organizations. This is a Priority I function and the question can only have a Yes or No answer. The scoring guidance is as follows:

- A [Yes] answer for this question can be achieved if all required [R] items are met.
- Any other combination of indicators is insufficient and results in a [No].

Note that if the detect activities are conducted by other external parties, incident management personnel or another organizational group must be sufficiently engaged and maintain a useful interface to have an accurate view of the organization's security posture as it relates to detection. If an established CSIRT exists, it is important that there is a defined interface through which the CSIRT can obtain this information.

Improvement – The optional or non-required indicators relative to network security monitoring identify areas where improvement in quality, timeliness, and accuracy can occur. This might include

- using automated tools
- ensuring automated alerts are enabled
- implementing multiple types of network monitoring systems
- ensuring results are analyzed in near real time
- ensuring network diagrams of monitoring system placement are available and up to date
- providing training to personnel on the various tools and methodologies being used

Incident Management Capability Metrics				
2. Detection				
2.1 Network Security Monitoring				
2.1.1	**Is there network monitoring of constituent systems and networks?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Network security monitoring is performed on all constituent networks.	Y ❑	N ❑

Prerequisites

- ❑ Permission to monitor constituents' networks has been acquired [R]
- ❑ There is an up-to-date, accurate, and complete list of all mission critical systems, data, and information [R]

Controls

- ❑ Criteria exist for characterizing anomalous events, including suspicious ports, protocols, services (both network based and host based) [R]
- ❑ MOU exists describing monitoring responsibilities of any third-party provider for constituent networks
- ❑ Documented policies and procedures exist that define how
  - constituent networks should be monitored and analyzed [R]
  - heuristic scanning is performed (as well as when) by IDS, AVS, and other network scanning tools
  - to review IDS logs, including a requirement for near "real-time" review
  - to request audit logs from constituents
- ❑ There is a strategy to ensure continuous network monitoring support to constituent networks and systems
- ❑ There are sufficient resources to ensure continuous network monitoring support to constituent networks and systems
- ❑ Personnel are appropriately trained on the procedures, process, and supporting technologies used to provide network monitoring and analysis, including log file analysis [R]

Activity

- ❑ Security monitoring is conducted on all constituent systems/networks [R]
- ❑ IDS or IPS on all constituent mission-critical networks is performed [R]
- ❑ Anomalous network events are characterized in support of network monitoring and intrusion detection
- ❑ Results of monitoring analysis are disseminated to appropriate individuals
- ❑ Logs are reviewed on a "real-time" basis or several times a day in order to detect possible intruders
- ❑ Reports or alerts/notifications are forwarded to other organizations as appropriate
- ❑ Low-level or heuristic events are routinely searched for and analyzed to identify possible unauthorized activity
- ❑ Copies of audit/system logs are requested within required timeframe of event detection to supplement analysis
- ❑ Monitoring data are analyzed on a regular basis (real-time, hourly, etc.)

Supporting Mechanisms

- ❑ Network monitoring tools, including network and host-based IDS or IPS [R]
- ❑ Monitoring tools have automated alert capability
- ❑ ADS system or an ADS plugin to an IDS system
- ❑ Behavior-based IDS for heuristic scanning for unauthorized activity
- ❑ Anti-virus software for heuristic scanning for malicious code detection
- ❑ Log analysis and correlation tools
- ❑ Alert capabilities exist, including appropriate communication mechanisms, such as page-out and email alerts
- ❑ Backup and recovery capabilities in the form of spare equipment for IDS sensors/console and other monitoring tools exist

Artifacts

- ❑ Samples of logs, alerts, and reports generated by the network monitoring tools [R]
- ❑ Network diagrams showing placement of monitoring tools on constituent networks
- ❑ Results of testing or monitoring on critical network segments [R]
- ❑ IDS configuration file specifying what anomalous events trigger an alarm

Quality Indicators

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Personnel are aware and knowledgeable about network monitoring tools and techniques, including how to review logs after detection of a potential incident [R]
- ❑ Constituents are aware of and knowledgeable about the network monitoring activities
- ❑ Criteria exist that define near-real-time as within _____ minutes/hours of detection (e.g., for review of logs)
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

[indirect]

FISMA Sec 3544(b)(7) [OLRC 2003]

3544(b) AGENCY PROGRAM - "Each agency shall develop, document, and implement an agency-wide information security program […] that includes […] (7) procedures for detecting […] security incidents […]"

Guidance References:

[counter reference – which provides guidance to the effect that another group, not the CSIRT, should perform this function]

NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]

Sec 2.5 Incident Response Team Services (intrusion detection responsibility should be assigned to another team)

[p 2-15] **Intrusion Detection**. "An incident response team may assume responsibility for intrusion detection because others within the organization do not have sufficient time, resources, or expertise. The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies. Ideally, however, primary responsibility for intrusion detection should be assigned to another team, with members of the incident response team participating in intrusion detection as their availability permits."

[indirect]

Sec 3.2.2 Signs of an Incident, and Sec 3.2.3 Sources of Precursors and Indications

NIST SP 800-31 *Intrusion Detection Systems* [Bace 2001]

Sec 2.2 Why should I use intrusion detection systems?

Internal Organization References:

2.2 Indicators, Warning, and Situational Awareness

2.2.1 Are network and system configurations or rule sets reviewed and updated in response to changes in the threat environment, and are the constituents notified of the updates?

This function focuses on whether the organization is able to quickly update and change network defense configurations and rule sets in a timely, structured manner to react to changes in the threat environment.

Not applicable – It is unlikely that this function would not be performed within the organization. To not perform this function is also ill advised. Failure to adjust network defenses to changes in threat environments could leave critical systems and data open to unauthorized access and exploitation. It is possible that this function might be handled by another part of the organization. If this is the case, then this question should be applied to that group and its activities. Incident management personnel should also have an established interface with the part of the organization with the authority to make these updates and also to other information sources that can provide indications of threat change levels.

Impact statement – Quickly making changes in network defense configurations in reaction to changing threat levels ensures that the organization can rapidly adjust its defenses and that the protection of critical systems and assets is at the highest level possible.

Scoring and interpretation guidance – This question is satisfactorily answered when the organization receives threat change information and is able to quickly adjust network defenses to protect against such threat changes while notifying constituents of the modifications and any resulting impacts. This is a Priority I function and the question can only have a Yes or No answer. Specifically, the scoring guidance is as follows:

- A [Yes] answer for this question can be achieved if all required [R] items are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – The optional or non-required indicators relative to configuration and rule set modifications indicate areas where improvement in quality, timeliness, and accuracy can occur.

Incident Management Capability Metrics				
2.2 Indicators, Warning, and Situational Awareness				
2.2.1	**Are network and system configurations or rule sets reviewed and updated in response to changes in the threat environment, and are the constituents notified of the updates?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ Configurations/rule sets are reviewed and updated in response to changes in the threat environment and the constituent is notified.	Y ❑	N ❑

Prerequisites

- ❑ There is access to information detailing changes in threat levels and environments [R]
- ❑ There is access to configurations and rule sets [R]
- ❑ Authority and responsibility for making network/system configuration and rule set updates is assigned [R]

Controls

- ❑ Documented policies and procedures exist that
  - define what types of changes in threat environments require changes to configurations and rule sets and the process for gathering that information and determining actions to be taken [R]
  - detail the process for IDS signature updates and the conditions that warrant updates
  - detail the process for updating router/firewall configurations (ACLs, logging, etc.)
  - define the process for notifying constituents of changes in the threat environment
- ❑ Personnel are appropriately trained on
  - the procedures, process and supporting technologies used in making configuration or rule set updates [R]
  - firewall rule sets, IDS and router configurations, and other appropriate or constituent-specific network defense configurations [R]

Activity

- ❑ Changes in the threat environment, e.g., threat and vulnerability reports/alerts, are monitored [R]
- ❑ Appropriate changes are implemented to IDS, router, firewall, and other appropriate network defense rules and configurations [R]
- ❑ Constituents are notified of modifications and impacts on constituent operations (increased IDS alerts, logs, loss of service, e.g., FTP port blocked) [R]

Supporting Mechanisms

- ❑ Vulnerability and threat monitoring mechanisms or methodologies [R]
- ❑ Information dissemination and communication mechanisms [R]
- ❑ Configuration and patch management systems and tools or methodologies [R]

Artifacts for Verification

- ❑ Documentation on when and why latest rule sets were updated
- ❑ Change log for configuration updates
- ❑ Copies of notification of changes and impacts [R]
- ❑ Up-to-date POC lists for constituents [R]

Quality Indicators

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Authorized personnel have knowledge and skills to make changes to appropriate monitoring devices [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: None [indirect] FISMA Sec 3544(b)(3) [OLRC 2003] 3544(b) AGENCY PROGRAM - "Each agency shall develop, document, and implement an agency-wide information security program, to provide information security for the information and information systems that support the operations and assets of the agency […] that includes […] (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"
Guidance References: None [indirect] NIST SP 800-41 *Guidelines on Firewalls and Firewall Policy* [Wack 2002] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-15] "**Technology Watch**. A team can perform a technology watch function […] The team should then make recommendations for improving security controls based on the trends that they identify."
Internal Organization References:

2.2.2 Is public monitoring of external security web sites and other trusted sources of information conducted?

This function focuses on whether the organization monitors security-related and general news sites in a structured manner to identify information that can be used to alert constituents to potential threats and problems. Part of this activity is the observation of new technical developments, new intruder activities, and related trends to help identify future threats. Topics reviewed can also include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can also include communicating with other parties who are authorities in these fields to ensure that the most accurate information or interpretation is obtained.

Such information might be used in daily briefings or shift change logs, as rationale for IDS signatures updates or changes in network monitoring configurations, as correlation information during incident or vulnerability analysis, as impetus for new training for incident management and constituent personnel, as a driver of new incident management research projects, or as information-sharing content sent to incident management staff.

Policies and procedures should identify the appropriate guidelines and rules for accessing and monitoring these sites, along with methods for extracting, synthesizing, and disseminating information.

Not applicable – It is possible that this function might be outsourced or handled by another part of the organization. If this is the case, this metric should be applied to that group and its activities. If this function is not performed anywhere within the organization or as an outsourced function, then a score of Not Applicable may be applied. However, note that this is a Priority I function, and it is considered a best practice. Performance of this function is critical to the effectiveness of the incident management capability.

Impact statement – Monitoring can provide early warnings about malicious threats or activity that may have an impact on the infrastructure. Monitoring may provide a better understanding of the significance, scope, and context of an event or incident, allowing response actions to be initiated in a timely manner to contain the potential damage and impact. This improves the overall network defense posture of the organization and allows it to have an agile response.

Scoring and interpretation guidance – This function is satisfactorily performed when the organization regularly monitors a variety of security, news, and other trusted sites for information relating to computing technologies, attacks, threats, and for socio-political, economic, or legal information that may be related to malicious computer security events and incidents. This is a Priority I function and the question can only have a Yes or No answer. Specifically, the scoring guidance is as follows:

- A [Yes] answer for this question can be achieved if all required [R] items are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement could be implemented through use of automated tools or intelligence agents to scan for specific types of information.

Incident Management Capability Metrics				
2.2.2	**Is public monitoring of external security web sites and other trusted sources of information conducted?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Public monitoring is conducted on a daily basis.	Y ❑	N ❑

Prerequisites

- ❑ Trusted external sources of information have been identified [R]

Controls

- ❑ Policies and procedures exist that detail how information is to be reviewed, collected, synthesized, disseminated, and used [R]
- ❑ A documented checklist exists that catalogs which sites to visit and critical information to examine each day [R]
- ❑ Documented safeguards and instructions exist for searching high-risk web sites such as "black-hat" sites in a safe, non-attributable or non-traceable fashion [R]
- ❑ Personnel are appropriately trained
  - on the procedures, process checklists, reliable web sites and supporting technologies used to perform information gathering or public monitoring [R]
  - in gathering and synthesizing information in a secure, safe manner [R]

Activity

- ❑ Personnel check a variety of web sites or email lists on a daily or weekly basis [R]
- ❑ Personnel extract and synthesize information gathered [R]
- ❑ Personnel communicate notable public monitoring information to appropriate technical and management staff and where appropriate, to the constituency [R]

Supporting Mechanisms

- ❑ Email systems and mailing lists
- ❑ Security, black hat, news, and legal web sites and archives
- ❑ Web search engines
- ❑ Mechanisms or methods to monitor, synthesize, and disseminate information [R]

Artifacts

- ❑ Records of gathered information [R]
- ❑ Web addresses for sites visited
- ❑ Archives of emails from mailing list subscriptions
- ❑ Reports synthesized based on the information gathered [R]

Quality

- ❑ Monitoring activities are automated or sources of information are automatically aggregated
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

[indirect]

FISMA Sec 3544(b) [OLRC 2003]

3544(b) AGENCY PROGRAM - "Each agency shall develop, document, and implement an agency-wide information security program, to provide information security for the information and information systems that support the operations and assets of the agency […] that includes […] (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Incident Management Capability Metrics
Guidance References: NIST 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-15] **Technology Watch**. A team can perform a technology watch function. Examples of this are monitoring security-related mailing lists […]"
Internal Organization References:

RESPOND: SECTION 3 OF INCIDENT MANAGEMENT CAPABILITY METRICS

In the Respond process, information that has been received by incident management personnel concerning potential incidents, vulnerabilities, or other computer security events or incidents is acted upon. This includes actions that may be performed by technical staff, management, or other entities within an organization. For example, technical actions can include

- analyzing the event or incident information, data, and supplemental material such as log files, malicious code, or other artifacts
- researching corresponding mitigation strategies and recovery options
- developing advisories, alerts, and other publications that provide guidance and advice for resolving or mitigating the event or incident
- containing any ongoing malicious activity by making technical changes to the infrastructure, such as disconnecting affected systems from the network, changing security configurations, or filtering ports, services, IP addresses, or packet content via firewalls, mail servers, routers, or other devices
- eradicating or cleaning up any malicious processes and files
- repairing or recovering affected systems
- providing assistance to constituents regarding response actions

Depending on the scope of the event or incident being handled, actions in the Respond process may be performed by a variety of people. For example, a CSIRT may perform initial incident analysis activities and provide guidance on responding to the incident but not be involved in performing containment, eradication, or recovery actions within the infrastructure. IT staff members or local system administrators may make those changes. But as all actions are in response to ongoing incident activity, they are considered part of the incident management process.

From a different perspective, management response highlights activities that require some type of supervisory or management intervention, notification, interaction, escalation, or approval as part of any response that is undertaken. Such management involvement may include actions taken by executive management or functional business managers such as human resources, legal counsel, public relations, financial accounting, audits and compliance, and other internal organization entities. Management response can also involve ensuring that various parts of the organization work together to handle events and incidents, and resolving any problems that occur between different parts of the organization.

Coordination must occur across all areas of the Respond process to be efficient and effective. All those involved in the response must communicate the steps that are being taken and any relevant information that needs to be disseminated. A response, such as a technical response, may require others to be involved. This type of cooperation and coordination should occur through established channels of communication that should be outlined in the policies, procedures, and plans associated with the Respond process. Actions are coordinated to ensure that efforts are not duplicated and that all tasks are completed within agreed-upon timeframes.

The Respond category includes the following subcategories:

Incident Reporting – incident management personnel and constituency understand the requirements for reporting and notification, information is appropriately managed, accessed, stored, archived, or destroyed

Incident Response – a 24x7 response capability exists and effective response processes are implemented, including involvement of appropriate individuals from technical, management, and other areas of the organization as required. Information is tracked and recorded, guidance is provided to constituency on how to report, incident management personnel build trusted relationships with internal organization experts and other external experts to facilitate response activities.

Incident Analysis – is conducted to determine the scope and impact of reported events and incidents and to determine the appropriate response strategies or workarounds to provide

3. Respond

3.1 Incident Reporting

3.1.1 Are incidents reported to and coordinated with appropriate external organizations or groups in accordance with organizational guidelines?

This function focuses on incident coordination and external communication. The primary focus is timely reporting of incidents to appropriate contacts in other organizations or groups. In addition, coordination with these groups or other CSIRTs to exchange and compare information is addressed here, although it is not a required activity. For example, in the U.S., at the federal government level, the Federal Information Security Management Act (FISMA) requires government agencies to report incident-related activities to US-CERT [OLRC 2003]. Some organizations in specific domains may have requirements for reporting incidents to a central reporting organization or may be part of a voluntary group of organizations pooling their incident information for greater effect.

Not applicable – If there is no requirement to report to an external group or organization, this function can be considered Not Applicable. Note that there may be other sector-specific requirements for reporting, such as disclosure of personally identifiable information that would make this function applicable.

Impact statement – If this function is performed well, then the communication channels and reporting chain(s) of the organization will support broad awareness. In other words, information gets to where it needs to be to enable effective and timely action in more than one organization.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization not only understands the requirements for reporting and coordination, but also submits requisite reports and shares information in a consistent, accurate, timely, and complete manner. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required indicators [R] are met.
- All other combinations of indicators yield a [No] answer.

Improvement – There are some non-required indicators that show where improvements could still be made, even if this metric is met. For example, activities for "coordinating with other CSIRTs" and "attending conferences, workshops, etc." if met, show that incident management personnel have the ability to effectively share information and work with external groups to expand their own views regarding incidents and help others achieve a broader understanding. They are active and contributing members of the global CSIRT community.

Having a cost-effective means of meeting reporting requirements (e.g., automated tools, templates, etc.) is not truly required for this metric, but would certainly improve the efficiency and eliminate costly manual efforts to produce reports. Implementing a centralized incident database that can also automatically produce the required reports is an excellent example of such an improvement.

Incident Management Capability Metrics				
3. Respond				
3.1 Incident Reporting				
3.1.1	**Are incidents reported to and coordinated with appropriate external organizations or groups in accordance with organizational guidelines?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Incidents are reported to and coordinated with other groups or organizations according to organizational guidelines.	Y ❑	N ❑

Prerequisites
- ❑ Guidance exists, including categories of incidents to report and required information [R]
- ❑ Reporting personnel are knowledgeable about the designated means of reporting incidents to appropriate entities (e.g., POCs, web site) [R]
- ❑ There is a designated department, group, or manager in the organization that has the responsibility for reporting incidents and the personnel work with that group or person [R]
- ❑ Documented requirements for levels of communications security exist [R]

Control
- ❑ Criteria exist for disseminating information [R]
- ❑ Documented criteria exist for what categories of incidents to report and the type of information to include [R]
- ❑ Documented policy exists for externally reporting incidents and coordinating/exchanging information with other CSIRTS [R]
- ❑ Documented procedures exist for reporting incidents to other relevant organizations including assigned roles and responsibilities and POCs [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity
- ❑ Personnel report incidents according to procedures and guidance directly or through an intermediate organization group [R]
- ❑ Coordination with other CSIRTS occurs to compare and exchange notes, analysis reports, and other information on intrusions, attacks, or suspicious activities within organization guidelines
- ❑ Personnel participate in workshops, conferences, working groups, technical exchanges, etc.

Supporting Mechanisms
- ❑ Forms (e.g., paper, email, web) for incident reporting along with instructions and examples [R]
- ❑ Documented, accurate POC list for other CSIRTS and/or intermediate internal group(s) [R]
- ❑ Secure communication mechanism to quickly disseminate intrusion information to appropriate constituents (e.g., PGP, GPG, S/MIME, PKI, secure FAX/STU, secure portal) with security commensurate for the sensitivity of the information [R]
- ❑ Cost effective means of meeting reporting requirements, (e.g., automated tools, templates, forms, or data collection mechanisms)
- ❑ Automated tools and processes for streamlined reporting and feedback

Artifacts
- ❑ Copies of reports sent to other groups or CSIRTs [R]
- ❑ Confirmation receipts from other groups when applicable [R]

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ❑ Information obtained from coordination is used to improve Defense-in-Depth layers (e.g., hot IP list, firewall ACL, etc.)

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(7)(B) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […] ''(7) procedures for detecting, reporting, and responding to security incidents […] including— […] ''(B) notifying and consulting with the Federal information security incident center referred to in section 3546 [US-CERT]"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.3.2.3 Incident Reporting [p 2-6] "FISMA requires Federal agencies to report incidents to [US-CERT] […]"
Internal Organization References:

3.1.2 Are incidents reported to appropriate organization management in accordance with organizational guidelines?

The purpose of this function is to ensure that the incident management personnel follow organization guidelines in reporting incidents (and/or events) within the organization. The objectives are to be able to demonstrate that appropriate notification is made to organization management using a repeatable, consistent, and reliable process that is well-documented, up to date, and understood by members of the team.

Not applicable – It would be highly unusual for this function to be Not Applicable as that would imply organization management has no interest. It is possible that this question applies to both an established CSIRT and an intermediate group/individual. An established CSIRT, for example, may report to an ISO, who then reports to other organization managers.

Impact statement – If this function is performed well, then the communication channels and reporting chain(s) of the organization will support broader awareness within the organization. In other words, information gets to where it needs to be to enable effective and timely action.

Scoring and interpretation guidance – Satisfactorily answering this question shows that incident management personnel are following organization management requirements for guidance on reporting. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required [R] indicators have been met.
- Any other combination of indicators yields a [No] answer.

Improvement – The optional quality indicators relative to gathering feedback and statistics are hallmarks of an organization that takes the time and effort to ensure that management assimilates information appropriately. In other words, incident management personnel check to determine if the reports are serving a useful function, and if not, work to improve them.

Incident Management Capability Metrics				
3.1.2	**Are incidents reported to appropriate organization management in accordance with organizational guidelines?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Incidents are reported internally to appropriate organization management according to organizational guidelines.	Y ❑	N ❑

Prerequisites

- ❑ Organization guidance (including criteria for what incidents to report, how to report, required content for report, and required timeframes) for internal reporting of incidents to organization management exists [R]

Control

- ❑ Policy defining what types of incidents should be reported and to whom exists [R]
- ❑ Documented procedures for reporting incidents internally to organization management exist [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Regular review of reporting guidelines with organization management is conducted, guidelines are updated as needed [R]

Supporting Mechanism

- ❑ Documented and up-to-date POC list with appropriate contact information and alternates [R]
- ❑ Defined mechanisms (e.g., forms, email, or telephone) used for incident reporting, along with instructions and examples [R]

Artifacts

- ❑ Copies of reports to management [R]
  - Tangible examples of reports to management from event/incident database or tracking system (daily/weekly/monthly)
- ❑ Sample organization management reports, showing accuracy of reported information

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References:

NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
3.2.7 Incident Notification
[p 3-16] "When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations. Timely reporting and notification enable all those who need to be involved to play their roles. […] Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates)."
Sec 3.5 Incident Handling Checklist
[p 3-26] Table 3-6. Generic Incident Handling Checklist of Uncategorized Incidents
Action 2. "Report the incident to the appropriate internal personnel and external organizations."
Sec 3.6 Recommendations
[p 3-28] "Include provisions regarding incident reporting in the organization's incident response policy. Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners."

Internal Organization References:

3.1.3 Are events/incidents reported from the constituency?

This function focuses on the communication from the constituency to the CSIRT or other incident management personnel designated as being responsible for receiving these reports as it relates to reporting events and incidents (e.g., the constituency discovers an event or incident and reports it). For this activity to occur in the most efficient way possible, defined, easy-to-use mechanisms for reporting events and incidents should exist. Such mechanisms facilitate the transfer of appropriate and useful information.

Not applicable – It would be unusual for this function to be Not Applicable, as that would imply the constituents never report events or incidents and incident management personnel only identify events and incidents through monitoring. The evaluator should capture the rationale for this function to be classified as Not Applicable and use judgment to decide whether the rationale is valid or not. If the reason is not valid, this question should be marked as not met.

Impact statement – If this function is performed well, then the communication channels and reporting chain(s) of the organization will support broader awareness within the organization. In other words, information gets to where it needs to be to enable effective and timely action.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that both the constituency and incident management personnel are familiar with reporting requirements, understand the types of activity to be reported (categories, reporting criteria, priorities, thresholds/triggers, etc.), and follow guidance on reporting. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required [R] indicators are met.
- All other combinations of indicators yields a [No] answer.

Improvement – Note that most of the indicators for this question are required, including the quality types of statistics. These statistics are critical if the organization is going to rely on the constituency to report accurate information. This does not mean that all constituents report all of the required information all of the time. A reasonable percentage should be established that provides the leeway for constituent reporting when incident management personnel must ask for more information or when the constituent simply does not have the required information. This indicator depends on the care with which incident management personnel define the information required for constituent reporting. If too much information is required from constituents, they may be discouraged from reporting. If too little information is required, incident management personnel will waste time contacting constituents to get additional data.

Incident Management Capability Metrics				
3.1.3	**Are events/incidents reported from the constituency?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ The constituency provides incident/event reports.	Y ❑	N ❑

Prerequisites

- ❑ Defined reporting parameters between constituency and appropriate incident management personnel exist (e.g., MOU, SLA, policy, or general knowledge) that specify any data or information that must be excluded, sanitized, or abstracted or have limited access [R]

Control

- ❑ Policy exists defining what types of events/incidents should be reported [R]
- ❑ Documented procedures exist for constituency reporting of events and incidents (including criteria for what events/incidents to report, how to report, required content for report, and required timeframes) [R]

Activity

- ❑ Guidance is provided to constituency on event/incident reporting requirements [R]
- ❑ Regular review of reporting guidelines with constituent is performed, guidelines are updated as needed

Supporting Mechanisms

- ❑ Forms/mechanisms used for constituent events/incidents reporting, along with instructions and examples (e.g., email, Web forms/instructions) [R]
- ❑ Documented and up-to-date constituent POC list with appropriate contact information and alternates [R]

Artifacts

- ❑ Copies of reports on file [R]

Quality

- ❑ Constituency understands the process for reporting events/incidents internally
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(7) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]

''(7) procedures for detecting, reporting, and responding to security incidents […]"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.3.1 Policy and Procedure Elements [p 2-3] "[…] requirements for reporting certain kinds of incidents" Sec 2.6 Recommendations [p 2-15] "Create an incident response policy and use it as the basis for incident response procedures. The incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items." Sec 3.5 Incident Handling Checklist [p 3-26] Table 3-6. Generic Incident Handling Checklist of Uncategorized Incidents Action 2. "Report the incident to the appropriate internal personnel and external organizations." Sec 3.6 Recommendations [p 3-28] "Include provisions regarding incident reporting in the organization's incident response policy. Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners."
Internal Organization References:

3.1.4 Is a notification service provided to constituents?

This function demonstrates whether the organization provides complete, abbreviated, or abstracted event or incident reports. In addition, it demonstrates how well warnings, notifications, alerts, and other information is provided to constituents to promote their awareness or to support response actions. Part of any effective incident management process is the ability to quickly disseminate the right information to the right people at the right time.

Not applicable – It would be unusual for this function to be Not Applicable as that would imply the incident management personnel never notify anyone in the organization about events or incidents. The evaluator should capture the rationale for this function to be classified as Not Applicable and use judgment to decide if the rationale is valid or not. If the reason is not valid, this question should be marked as not met.

Impact statement – Involvement in the notification service ensures timely information is received by constituents to alert them to security situations that could affect operations or business functions of the organization. This enables them to respond to threats, vulnerabilities, or other malicious activity.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the CSIRT provides an adequate notification service to its constituents. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required [R] indicators are met.
- All other combinations of indicators yields a [No] answer.

Improvement – The only non-required indicators refer to improvements that could be made by defining specific criteria for the quality of the notifications sent to constituents and gathering information from constituents that can be used to provide needed improvements to the content, mechanisms, timing, or delivery of notifications. Without such information, incident management personnel may not know that they are not providing what constituents need.

Incident Management Capability Metrics				
3.1.4	**Is a notification service provided to constituents?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ A notification service is provided to the constituency.	Y ❑	N ❑

Prerequisites

- ❑ Documented requirements exist for levels of communications security [R]
- ❑ Criteria exist for disseminating information exist, defining who receives what data and when [R]

Control

- ❑ Documented policies exist that define the types of notification given to constituents including [R]
  - events/incidents, including what types
  - general and specific threat warnings and notifications
  - official threat reports
  - organization-specific levels of awareness/risk/impact associated with threat/vulnerabilities
  - countermeasures or interim guidance for threats/vulnerabilities
- ❑ Documented tactics, techniques, and procedures for notifying constituency exist including
  - how to notify [R]
  - required content for notifications [R]
  - required timeframes [R]
  - relaying threat reports that emphasize Need to Know
  - assessing level of risk relative to organization and explaining impact [R]
  - screening and filtering reports
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Potential impact of threats and vulnerabilities to constituents are analyzed and distributed [R]
- ❑ Pre-defined countermeasures or protection strategies are documented and distributed, if required
- ❑ Notifications are sent to appropriate constituents [R]
- ❑ Regular review of reporting guidelines with constituent are performed and guidelines are updated as needed [R]

Supporting Mechanisms

- ❑ Mechanisms exist, along with instructions and examples, for reporting events/incidents to constituents (e.g., email, Web, mailing lists, etc.) [R]
  - secure communication mechanism to quickly disseminate intrusion information to appropriate constituents commensurate with the sensitivity of the information (e.g., PGP, GPG, S/MIME, PKI, secure FAX/STU, secure portal) [R]
- ❑ Documented and up-to-date constituent POC list with appropriate contact information and alternates [R]
- ❑ Documented sources for information gathering on alerts and warnings [R]

Artifacts

- ❑ Copies of threats, warnings, event/incident reports, etc. [R]
- ❑ Valid, up-to-date POC information for notifications [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec. 2.5 Incident Response Team Services [p 2-14] "**Advisory Distribution**. A team may issue advisories that describe new vulnerabilities in operating systems and applications and provide information on mitigating the vulnerabilities. Promptly releasing such information is a high priority because of the direct link between vulnerabilities and incidents. Distributing information about current incidents also can be useful in helping others identify signs of such incidents. It is recommended that only a single team within the organization distribute computer security advisories, to avoid duplication of effort and the spread of conflicting information." [indirect] Sec 3.2.7 Incident Notification [p 3-16, 3-17] "When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations. Timely reporting and notification enable all those who need to be involved to play their roles. […] Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates). […] During the handling of an incident, the team may need to notify certain parties frequently of the current status of the incident. In some cases, such as a major malicious code infection, the team may need to send organization-wide updates. The team should plan and prepare several communication methods, and select the methods that are appropriate for a particular incident. For example, if the email server has been overwhelmed by malicious code, the team should not send incident updates by email. Possible communication methods include—Email; Web site (Intranet-based); Telephone Calls; In person (e.g., daily briefings) Voice mailbox greeting […]; Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)."
Internal Organization References:

3.1.5 Are incidents reported to law enforcement as required and/or the intelligence community as appropriate?

This function demonstrates whether the organization reports the appropriate types of activity to law enforcement (LE) or to the intelligence community (IC) as required. Information reported should include the timeframes, details, and any other relevant information. Law enforcement may have different reporting requirements from the intelligence community, so it will be important for any organization to determine when it should report to either area and the exact reporting process and points of contact.

Note that intelligence community reporting may not always be a requirement for some organizations. There may be indirect reporting and communication mechanisms, through a legal representative or senior management, for example. In that case, this function applies to both the incident management personnel for reporting to the intermediate group/person and to the intermediate group/person for reporting to law enforcement.

Not applicable – If only law enforcement reporting is required, then the words "intelligence community" can be ignored. In some jurisdictions, reporting to law enforcement may be a requirement, for example, when evidence of certain types of crime is revealed during investigation of an incident.

Impact statement – Some organizations may be required to report different types of activities to these entities and failure to do so may result in penalties or other consequences as defined by these entities or other regulations.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization meets the needs of the law enforcement and/or intelligence community with respect to the reporting of incidents within the organization. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required [R] indicators are met.
- All other combinations of indicators yields a [No] answer.

Improvement – Improvements can be made by

- providing templates or forms to ensure consistent reporting if these are not provided by law enforcement or the intelligence community
- gaining confirmation of the receipt of reports where possible, to verify that the communication mechanisms are working properly
- arranging assignment of a specific case number and investigator(s) to successfully transitioned reports
- gathering information in a "forensically sound" manner

Incident Management Capability Metrics				
3.1.5	**Are incidents reported to law enforcement as required and/or the intelligence community as appropriate?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Incidents are reported to law enforcement and/or intelligence communities as appropriate.	Y ❑	N ❑

Prerequisites

- ❑ Guidance from law enforcement and intelligence community exists, including categories of incidents to report and required information, timeframes, and contact mechanisms [R]

Control

- ❑ Policies, procedures, and training materials are consistent with latest guidance from law enforcement and intelligence community [R]
- ❑ Documented policy exists for requiring certain incidents to be reported to appropriate law enforcement and/or intelligence community [R]
- ❑ Documented procedures exist for reporting incidents to law enforcement and intelligence community including [R]
  - assigned responsibility and/or POC in the organization or CSIRT
  - documented methodology for sharing information with the intelligence community via proper channels
  - evidence handling per law enforcement/intelligence community requirements
  - incident categories for reporting including the type of information to provide
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Contact is maintained with appropriate LE/IC POCs for changes in reporting requirements [R]

Supporting Mechanisms

- ❑ Communication channel or mechanism for reporting [R]
- ❑ Forms for incident reporting along with instructions and examples
- ❑ STU III, secure FAX, PGP, GPG, S/MIME encrypted email, PKI, or other suitable mechanisms for secure information sharing [R]

Artifacts

- ❑ Copies of reports to LE/IC or to intermediate group [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ Confirmation is received from law enforcement and intelligence community when applicable
- ❑ LE has assigned a case number and handler to this incident as indication of successful hand-off
- ❑ There is a process and criteria (such as consistency with law enforcement or intelligence community reporting requirements) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(7)(C)(i) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]

''(7) procedures for detecting, reporting, and responding to security incidents […] including— […]

''(C) notifying and consulting with, as appropriate—

''(i) law enforcement agencies and relevant Offices of Inspector General"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.3.2.2 Law Enforcement [p 2.5, 2-6] "The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected. Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures."
Internal Organization References:

3.1.6 Is there support for incident management for classified or sensitive information, networks, and/or systems?

If incident management personnel provide classified or other sensitive incident management services, it is imperative that mechanisms and processes be in place to handle the information at the appropriate level of classification/sensitivity. They will need to know what information is sensitive or classified and where it exists or is transmitted on systems and networks. The constituents will need to know how to properly report events and incidents involving sensitive or classified information, systems, or networks. The evaluator may need appropriate clearances to be able to view, confirm, or validate that the question has been satisfied. Otherwise, incident management personnel must be able to provide sufficient detail (without providing access to classified/sensitive networks, data, or information) to provide confirmation of the existence of appropriate handling of such elements.

Not applicable – Although not all organizations may need to deal with classified information, all will have some types of information that is considered sensitive; even if it is only employee social security numbers and salary information. Therefore, this function should never be considered Not Applicable. If the organization believes this is truly not applicable, then proper documentation of this rationale is required.

Impact statement – Ensuring that mechanisms are well understood and in place for handling sensitive or classified data or information will prevent unauthorized disclosure of such information.

Scoring and interpretation guidance – The goal of this question is to assure that the organization has established incident management policies, procedures, and communication mechanisms in place commensurate with the sensitivity or classified nature of the information/data. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory answer for this question [Yes] can be achieved only if all of the required [R] indicators have been met.
- Any other combination of indicators yields a [No] answer.

Improvement – For this question, one of the non-required indicators that can be an improvement relates to implementing a "decision matrix or mechanism that can be used to quickly assign proper classification or sensitivity levels." Such a mechanism can certainly improve efficiency when sensitive or classified information is relatively common, but produces less return on investment when such information is sparse.

Incident Management Capability Metrics				
3.1.6	**Is there support for incident management for classified or sensitive information, networks, and/or systems?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ Incident management for classified or sensitive information is supported.	Y ❑	N ❑

Prerequisites

- ❑ There is a documented list of networks/systems which support classified or sensitive information [R]
- ❑ Defined levels or schemes of sensitivity/classification for data and information exist as appropriate [R]
- ❑ Documented requirements exist for levels of communications security [R]

Control

- ❑ Documented policy exists for managing incidents involving networks supporting sensitive or classified information [R]
- ❑ Documented procedures cover all aspects of incident management, including external and internal reporting, response, the required means of communicating, specified markings for level of sensitivity/classification, any variations for different levels of sensitivity/classification, use of encryption, using secure communication channel [R]
- ❑ Personnel are appropriately cleared for the applicable levels of sensitivity of networks/systems/information [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Incident reports are categorized and protected in accordance with appropriate organization regulations [R]
- ❑ Incidents involving sensitive or classified information are handled according to organization guidelines [R]
- ❑ Data and information have been assigned and labeled according to the appropriate class or category of sensitivity [R]

Supporting Mechanisms

- ❑ Secure communications channel (STU/STE, secure FAX, etc.) for incidents involving classified or sensitive information that are protected up to the level of classification/sensitivity of that information [R]
- ❑ Secure storage/repository appropriate to the levels of sensitivity/classification [R]
- ❑ Defined access lists for associated classifications [R]
- ❑ Encryption techniques that meet NIST or other national or international regulations
- ❑ Decision matrix or mechanism for quickly assigning proper classification of event/incident data and reports

Artifacts

- ❑ Sample, sanitized incident reports on classified or sensitive information or systems [R]
- ❑ Classification/sensitivity level clearly marked on reports [R]
- ❑ Classified or sensitive reports are stored at the level of their classification [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently perform the procedures [R]
- ❑ Constituents are aware and knowledgeable of the procedures for incidents involving sensitive or classified information
- ❑ Clearance records on file for personnel (100% for cleared personnel and those in intermediate status (e.g., pending)) [R]
- ❑ There is a process and criteria (such as consistently appropriate management of sensitive/classified information) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: FISMA Sec 3544(b)(7) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […] ''(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b) [National Security Systems] […]"
Guidance References: None [indirect] NIST SP 800-59 *Guideline for Identifying an Information System as a National Security System* [Barker 2003]
Internal Organization References:

3.1.7 Is there a central repository for constituent security event/incident reporting?

This function gauges the ability of the CSIRT or incident management personnel to serve as a repository (clearinghouse) to collect and archive data on events and incidents reported by constituents. Such a repository supports the collection and storage of historical information. This information can then be easily searched for common intruder signatures and attacks, relevant mitigation and resolution strategies, and historical trends.

Not applicable – In some organizations with distributed incident management responsibilities, a CSIRT may function more as a coordinator, with individual groups or departments maintaining their own repositories of event and incident data. In this case, this function may be Not Applicable or it may be applied to all groups retaining some portion of the event/incident information.

Impact statement – This consolidated data can be used as a source for any fusion or retrospective analysis that may be done (discussed further in Section 3.3). Performing these types of analysis enables incident management personnel to obtain a broader view of ongoing incident activity and compare it against other external observations or activity.

Scoring and interpretation guidance – For this priority II function, there should be the tools, techniques, and processes to collect, protect, and appropriately store the information/data, as well as the ability to easily access and extract content for a variety of needs (statistics, reports, types of reports, organizations/sites, status, etc.).

- The [Yes] answer for this question can be achieved if all of the required [R] indicators are met.
- The organization can obtain a [Partial] answer on this question if all of the required [R] indicators are met EXCEPT in regard to keeping all information as required. For example, if an organization only retains information on confirmed incidents or only keeps some of the event/incident reports for the required timeframe and some is purged too early, only a partial score could be achieved.

Improvement – For this function, one possible improvement that could be made even after the metric is met would involve gathering and analyzing quality statistics on record retention and using an off-site or alternate site for archival of records. Off-site archival is easier to achieve with a centralized database or knowledge base for events and incidents but may be more difficult if the data is distributed.

Incident Management Capability Metrics						
3.1.7	**Is there a central repository for constituent security event/incident reporting?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ ALL event/incident reports (electronic and/or paper) are retained for the required time period.	Y ❑	P ❑	N ❑
		Partial	▪ SOME event/incident reports (electronic and/or paper) are retained for the required time period but the approach is inconsistent.			

Prerequisites
- ❑ Policy or procedures dictate the centralized receipt of constituent event/incident reports [R]
- ❑ Constituents report events/incidents to the designated group [R]

Control
- ❑ Documented policy exists defining organization guidelines for record retention [R]
- ❑ Documented procedures for archiving, retiring, and destroying records exist [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity
- ❑ All of the event/incident reports from constituents are retained according to requirements in either paper or electronic form [R]
- ❑ Archived reports are encrypted (if electronic)
- ❑ All reports are backed up [R]

Supporting Mechanisms
- ❑ Record repository with controlled access [R]
- ❑ Alternate site for archiving records
- ❑ Backup systems or mechanisms [R]

Artifacts
- ❑ Sample event/incident reports from constituents from repository [R]
- ❑ Schedule for backup or archival of reports

Quality
- ❑ Personnel are aware and knowledgeable of the procedures [R]
- ❑ Personnel consistently follow the procedures [R]
- ❑ Event/incident reports are archived for at least one year or in accordance with organization guidelines or industry best practices [R]
- ❑ There is a process and criteria (such as required storage timeframe, appropriate destruction of records, and completeness, accuracy, and timeliness of constituent reporting) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References:

NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 3.2.5 Incident Documentation
[p 3-13, 3-14] "As soon as an incident response team suspects that an incident is occurring or has occurred, it is important to immediately start recording all facts regarding the incident. […]
The incident response team should maintain records about the status of incidents, along with other pertinent information. […]
The incident response team should take care to safeguard data related to incidents because it often contains sensitive information—for example, data on exploited vulnerabilities, recent security breaches, and users that may have performed inappropriate actions. To reduce the risk of sensitive information being released inappropriately, the team should ensure that access to incident data is restricted properly."

Internal Organization References:

3.2 Incident Response

3.2.1 Is there an event/incident handling capability?

Having an effective event/incident handling capability means the appropriate people, processes, and techniques are in place and established to support the activity. The event/incident handling capability in this metric addresses the basic aspects for incident management: for example, handling events and incidents that incident management personnel find and that constituents report; 24x7 capability of some kind; communication and coordination of incident response; appropriate escalation of events and incidents; and optional on-site support to constituents.

Not applicable – To have an incident management capability of any depth, this function will always be applicable to someone or some group in the organization, even if it is not a CSIRT. Therefore, Not Applicable is not an option.

Impact statement – Any organization that has networked systems connected to the internet must be able to handle events and incidents—even if the service is outsourced to a third party. Such a capability will enable the organization to understand the types of probes, threats, events, and incidents that affect the organization's overall "wellness"; without such a capability, the risk to the business, products, services, financial situations, and trust can all be affected.

Scoring and interpretation guidance – The goal of this question is to assess whether the organization can provide adequate incident management services. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer can be achieved only if all of the required [R] indicators are met. This is a complex question and there are many ways some of the activity indicators could be met. Additional guidance is as follows.
  - A 24x7 capability does not require a full-time physical presence. Incident management staff should be available and accessible—on call—if the need arises. Staff can be contacted via pager, mobile phone, email, etc. There could be assigned shifts. All personnel must understand the types and scope of support and how to contact people during various shifts. In addition, there should be criteria for triggering different levels of support (e.g., when people need to report to work off-shift). Roles and responsibilities, minimal response times, and management of shift changes should be defined.
  - Criteria or procedures for escalation should define how and when to escalate, to whom, and any required approvals.
  - On-site support can be provided in a variety of ways, including remote monitoring with telephone support, sending personnel to a different building, or traveling to a different geographic facility. Constituents must know the nature of the support, the circumstances for getting it, and the applicable timeframes (e.g., two days for traveling across the country).
  - The mechanism used to support event/incident handling can be simple or complex (e.g., email folders, separate files, spreadsheet, automated tool or database, or customized software) but it does need to meet the organization's needs, be appropriately managed

and controlled (like any other critical application or tool), and be able to scale up or adapt to changing conditions. The mechanism should

- provide reports such as incident type/category/severity, incident activity summary, events/incidents, affected sites list, action lists, administrative statistics
- retain event/incident data, at a minimum, as required by the organization for incident reporting
- be documented in up-to-date user guides
- have sufficient backup capability, including its data content
- be easily used and adapted to changing requirements, threats, or increased events/incidents
- be consistent, reliable, interoperable (e.g., can import/export data internally and externally from organization), and available (backups for data and software, off-site data centers, swaps, etc.)
- be developed, documented, and maintained per the organization's software/system development life cycle requirements with full hardware/software support for maintenance available

Improvement – There are some non-required indicators for this function that can be considered indicators for improved or higher quality service. They have to do with either quality assurance of the incident handling products or gathering feedback from constituents and other parts of the organization on the quality of the incident handling activities. Gathering and acting upon such information is essential to maintaining high levels of constituent satisfaction and continuing to maintain and improve the security posture of the organization. This activity can be done without such information, but without feedback incident management personnel run the risk of eventually failing in their duty to their constituents and the organization.

Incident Management Capability Metrics				
3.2 Incident Response				
3.2.1	**Is there an event/incident handling capability?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is an event/incident handling capability.	Y ❑	N ❑

Prerequisites

- ❑ CSIRT has current lists of constituent mission critical systems, data, and information [R]
- ❑ Clearly documented communication channels exist that define who is to receive or provide what information when, and under what circumstances, and in what timeframe for handling events/incidents [R]
  - If constituents or other parts of the organization are responsible for some or all of the incident response activities, there are defined roles and responsibilities (e.g., SLAs, MOUs, email)
- ❑ Documented guidelines, thresholds, or criteria for when to escalate events/incidents exist [R]

Control

- ❑ Documented event/incident handling policies and procedures exist, including [R]
  - provided services
  - any relevant criteria and limitations
  - clearly defined roles and responsibilities
  - guidelines for 24x7 support, special instructions for critical systems, and response time goals based on at least the category/severity of threat/incident
- ❑ Personnel are appropriately trained on the procedures, technology, and tools used in this activity [R]
- ❑ Constituents are provided with documentation that outlines incident handling services, (e.g., in SLA, MOU, email, web page announcement, etc.) [R]

Activity

- ❑ All event/incident reports are reviewed and a decision is made about how to respond [R]
- ❑ All events/incidents reported by constituents are responded to or at least those that have been identified as possibly affecting constituent systems [R]
- ❑ Event/incident responses are escalated as required [R]
- ❑ Incident response activities are coordinated with constituents or other parts of the organization as needed [R]
- ❑ On-site support for incident response is provided

Supporting Mechanisms

- ❑ Mechanisms to track incidents and support the response process appropriate to the number/complexity of organization events/incidents [R]
- ❑ Mechanisms to support transition of current activities across shift changes, e.g., status boards, hand-off reports, etc. [R]
- ❑ Up-to-date contact information for all POCs and alternates (for CSIRT staff, SMEs, notification lists, constituent sites, ISOs, etc.) for all shifts, critical information/systems, constituents, others performing incident handling activities [R]
- ❑ Toolkit for on-site support
- ❑ Web sites (or other communication mechanisms such as phone or email) [R]

Artifacts:

- ❑ Sample event and incident reports [R]
- ❑ Escalation requests or escalated events/incidents log showing timeframes were met
- ❑ Sample reports generated by tools
- ❑ Data entry pages or interfaces
- ❑ After action reports from on-site support

Incident Management Capability Metrics
Quality: ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, technology, and processes [R] ❑ Constituency understands the nature of the services provided and their responsibilities ❑ Other parts of the organization understand their roles and responsibilities ❑ There is a process and criteria (such as timeliness, accuracy, completeness, and usefulness of the response) for evaluating the quality of performance and artifacts associated with this activity [R] ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
Regulatory References: FISMA Sec 3544(b)(7) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […] ''(7) procedures for detecting, reporting, and responding to security incidents […]" OMB Cir A-130 App III Sec A.3.a.2)d) Incident Response Capability "Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance."
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.2 Need for Incident Response [p 2-2] "Incident response has become necessary […] Federal departments and agencies must comply with law, regulations, and policy directing a coordinated, effective defense against information security threats." Sec 2.4 Incident Response Team Structure [p 2-8] "An incident response team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred." Sec 2.6 Recommendations [p 2-15] "**Establish a formal incident response capability**. Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities."
Internal Organization References:

3.2.2 Is there an operations log or record of daily operational activity?

This function focuses on whether a CSIRT (or incident management personnel) tracks and records the current state of operations and activities on a daily basis. While an operations log is one commonly used method of recording such information, other mechanisms may include blogs, instant messaging, bulletin boards, or white boards. This is an essential part of managing activities across time shifts, passing down information to incoming personnel, or enabling people to coordinate and communicate, particularly for those incidents that involve weeks or even months of activity. Information in operations logs can include data or status on events/incidents that are open, closed, or unresolved, current advisories and alerts, current IDS data, and so on.

Not applicable – Depending upon the nature of the 24x7 incident management support and the complexity and capability of incident management personnel's knowledge bases, some type of information capture should exist. If this function is deemed not applicable, documentation on the rationale should be captured.

Impact statement – Without such a daily record, there is no way to adequately assess incident management activities that occur.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that incident management personnel have a well-maintained, complete operations log. Partial satisfaction would be an incomplete log. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved only if all of the required [R] indicators are met. Remember that the operations log can be as simple as a paper-based log book, but it should be available for viewing.
- The [Partial] grade for this question can be achieved if all of the required [R] indicators are met BUT a review of the operations log shows it is not complete or has incorrect entries—an indication that procedures are not being followed and that the log is probably not being reviewed for correctness.

Improvement – The other non-required indicators relate to the quality improvements that can be achieved if metrics or quantifiable criteria for quality exist and are used to measure the effectiveness and usefulness of the operations log. Another optional indicator that the evaluator can observe is the actual shift change to determine if procedures are being followed.

Incident Management Capability Metrics						
3.2.2	**Is there an operations log or record of daily operational activity?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ There is an operations log. Entries are up to date and complete.	Y ❑	P ❑	N ❑
		Partial	▪ There is an operations log, but entries are missing or incomplete.			

Prerequisites

- ❑ None

Control

- ❑ Documented procedures specify how the log is maintained and reviewed, who is authorized to enter what data, who is authorized to edit the log, who is authorized to see the log, and the information that is required in the log [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Operations log or record includes daily operations tracking and recording, shift change transitions, and the current state of activity [R]
- ❑ Operations log is accessible by all appropriate personnel
- ❑ Personnel are informed of the significance of the log [R]

Supporting Mechanisms

- ❑ Tools or technology to support and maintain daily operations log (e.g., paper, automated incident database, electronic status board, blogs, spreadsheet, shift change briefings, etc.) [R]

Artifacts

- ❑ Incident handling operations log (soft and/or hardcopy) for review showing entries are up to date and complete and transition across shifts is supported and documented [R]

Quality

- ❑ Personnel responsible for the operations log are aware of, knowledgeable of, and consistently follow the procedures for this activity [R]
- ❑ The operations log is reviewed periodically for completeness, correctness, and quality of information [R]
- ❑ Document, report, or tool is adaptable and useful for providing needed information in timely manner
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References: None

Internal Organization References:

3.2.3 Is information on all events/incidents collected and retained in support of future analytical efforts and situational awareness?

This function focuses on whether the right set of information on events and incidents is collected and retained to support analysis and situational awareness. Events are included here as some incidents are only declared after review of different events yields a pattern of activity or behavior that indicates an incident.

Not applicable – If a CSIRT is not the central repository of event/incident information and no other group is acting in this capacity, this function is Not Applicable. However, this does leave the organization vulnerable to future incidents that may have been prevented had someone been able to analyze all of the data, improve situational awareness, and conduct the "low and slow" types of analyses that identify the more subtle forms of attacks.

Impact statement – This type of analysis can be essential for identifying "low and slow" attacks and managing such incidents.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization maintains information on all events and incidents (not just a select few and not just incidents). This is a priority II function.

- The [Yes] answer for this question can be achieved only if all of the required [R] indicators are met.
- The [Partial] grade for this question can be achieved if the required [R] indicators are largely met, but not all of the information for an event or incident, or not for all of the event/incidents, is collected and retained. For example, an organization that only retains incident data could get a partial score, as could a CSIRT that retains both event and incident data, but only for a portion of the organization.

Improvement – Encryption is an improvement for retaining information and would help meet other metrics associated with maintaining confidentiality of sensitive information. Tracking retention rates to ensure guidelines are met would be another improvement. Implementing automated tools that help in correlation of data and analysis would also be improvements.

Incident Management Capability Metrics						
3.2.3	**Is information on all events/incidents collected and retained in support of future analytical efforts and situational awareness?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ Information on all events/incidents is maintained for future analytical efforts and situational awareness.	Y ❑	P ❑	N ❑
		Partial	▪ Some information is maintained on some events/incidents.			

Prerequisites

- ❑ None

Control

- ❑ Policy exists stating the required period of retention for events and incidents, with reference to the relevant organizational requirements or guidelines [R]
- ❑ Procedures for event/incident data collection and retention exist [R]
- ❑ Guidelines/procedures for secure handling, storage, transmission, and destruction of event/incident data exist [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity

- ❑ Data is retained for a period of at least one year or in accordance with organizational guidelines [R]

Supporting Mechanisms

- ❑ Repository – soft and/or hard copy – of event/incident data [R]
- ❑ Encryption techniques to store data in the repository

Artifacts

- ❑ Sample records from the repository [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ Periodic review of secure repository for adequacy of security occurs
- ❑ Periodic review of retained records occurs to verify timeframes are followed
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity (including verification of retention timeframes and adequacy of security of the repository)are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

General Records Schedule 24 – *Information Technology Operations and Management Records* [NARA 2003]
7. Computer Security Incident Handling, Reporting and Follow-up Records.
"Destroy/delete three years after all necessary follow-up actions have been completed."
[indirect]
FISMA Sec 3544(b)(7)(C)(i) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
''(7) procedures for detecting, reporting, and responding to security incidents […] including— […]
''(C) notifying and consulting with, as appropriate—
''(i) law enforcement agencies and relevant Offices of Inspector General"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.5 Incident Documentation [p 3-13, 3-14] "As soon as an incident response team suspects that an incident is occurring or has occurred, it is important to immediately start recording all facts regarding the incident. […] The incident response team should maintain records about the status of incidents, along with other pertinent information. […]" Sec 3.4.2 Using Collected Incident Data [p 3-23] "Over time, the collected incident data should be useful in several capacities. […] A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changed in incident trends."
Internal Organization References:

3.2.4 Is relevant information on all events/incidents collected and retained in support of law enforcement investigations?

This function focuses on whether the right set of information on events and incidents is collected and retained to support law enforcement investigations. Retention of event/incident information can support law enforcement investigations that could lead to successful prosecution of criminal activities. The ability to reference data collection and analysis that can be accepted in a court of law is critical to success in such organizations. Without such information, the organization cannot prosecute because there is insufficient data or it is corrupted and inconclusive.

Not applicable – This function should never be considered "not applicable" to an organization or a CSIRT. However, if an organization regards this as Not Applicable, there must be supporting policy documentation stating that the organization chooses not to support law enforcement investigations relating to events and incidents.

Impact statement – Properly collected and retained information is an essential part of criminal prosecution.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization maintains information on all events and incidents (not just a select few and not just incidents) in a forensically sound manner. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer can be achieved if all of the required [R] indicators have been met. Note that in the absence of specific guidance from local law enforcement, the organization may have to make its best, educated guess or find guidance from its legal representatives on chain-of-evidence and other law enforcement requirements. The evaluator may need to use some judgment to determine if an organization has done all that it can to create a reasonable set of policies, procedures, and guidelines to meet this function.

Improvement – Documentation from law enforcement that describes its information requirements would serve as an excellent reference, but it may not always be available. Using encryption can be one means of maintaining confidentiality and integrity. As the time required to retain information in support of legal matters can be quite lengthy, actually verifying this is being done correctly may be critical to supporting the chain of evidence.

Incident Management Capability Metrics				
3.2.4	**Is relevant information on all events/incidents collected and retained in support of law enforcement investigations?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ Information on all events/incidents is maintained for law enforcement/criminal investigation efforts.	Y ❑	N ❑

Prerequisites
- ❑ None

Control
- ❑ Policy exists stating the required period of retention for events and incidents, with reference to the relevant law enforcement guidelines [R]
- ❑ Guidelines/procedures exist for
  - event/incident data collection and retention [R]
  - secure handling, storage, transmission, and destruction of event/incident data [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity
- ❑ Data is retained for a period of at least one year or in accordance with organization and law enforcement guidelines [R]
- ❑ Periodic reviews of secure repository for adequacy of security are conducted
- ❑ Information is collected in a forensically sound manner to support law enforcement

Supporting Mechanisms
- ❑ Repository (and backup) – soft and/or hard copy – of event/incident data is used that supports chain-of-custody requirements [R]
- ❑ Encryption techniques used to store data in the repository

Artifacts
- ❑ Records from the repository [R]
- ❑ Documents or input from local law enforcement on what information is needed and other requirements

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness (such as adherence to retention timeframes and appropriateness of protection measures) of this activity are periodically evaluated (and appropriate improvements are made [R]

Regulatory References:
General Records Schedule 24 ─ *Information Technology Operations and Management Records* [NARA 2003]
7. Computer Security Incident Handling, Reporting and Follow-up Records.
"Destroy/delete three years after all necessary follow-up actions have been completed."
[indirect]
FISMA Sec 3544(b)(7)(C)(i) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
''(7) procedures for detecting, reporting, and responding to security incidents […] including— […]
''(C) notifying and consulting with, as appropriate—
''(i) law enforcement agencies and relevant Offices of Inspector General"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.3.2.2 Law Enforcement [p 2-5] "The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss […] what evidence should be collected, an how it should be collected." Sec 3.2.5 Incident Documentation [p 3-13] "Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued." Sec 3.3.2 Evidence Gathering and Handling [p 3-18] "[…] it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies, so that it should be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence […]" Sec 3.4.3 Evidence Retention [p 3-25] "**Prosecution**. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished. **Data Retention**. Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that email messages should be retained for only 180 days. If a disk image contains thousands of emails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary. As discussed in Section 3.4.2, General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years."
Internal Organization References:

3.2.5 Are general incident response guidelines, checklists, and recommended procedures distributed to constituents to encourage consistency in response methods/standards?

This function focuses on how general guidelines, checklists, and other information are provided in order for to constituents to encourage consistent response to identified incidents. To do this well, incident management personnel should not simply acquire recommended response strategies from other sources and convey them to the constituents. General guidance from other sources should always be reviewed for relevance and applicability to the organization. Organization-unique guidance should also be developed and maintained. Constituents may not be as knowledgeable as incident management personnel on the best methods for testing and installing patches, changing configurations, or implementing workarounds and other mitigation strategies.

Not applicable – This particular activity may not be applicable if, for example, a formal CSRT performs all of the response activities. If this function is deemed not applicable, the rationale should be documented and the evaluator should judge if the rationale is sufficient.

Impact statement – By providing guidelines and recommendations for taking response actions, incident management personnel can help the constituency implement a complete response in a more effective and efficient manner.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that up-to-date guidance and checklists are built, acquired, and maintained, and routinely distributed to constituents. A partial answer for this question could be met if the guidance is distributed periodically. Specifically, the scoring guidance is as follows:

- The [Yes] answer for this question can be achieved only if all of the required [R] indicators have been met.
- The [Partial] grade for this question can be achieved if the required indicators have been met with the exception of any of the following:
  - Guidelines, checklists and other information are distributed on a random basis that does not provide up-to-date information to constituents.
  - Guidelines, checklists, and other information is acquired from other sources and passed to constituents without review or modification (or constituents are pointed to other sources and told to find information on their own).
- If there are neither informal nor formal documented procedures, then the answer is [No].

Improvement – As a means of improvement to this activity, feedback from the constituents on the usefulness of the information should be gathered and analyzed. In addition, using multiple means of delivering the information is preferable to relying on a single communication mechanism. Choose the mechanism most appropriate to the nature of the information being conveyed.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>3.2.5</td><td colspan="4">Are general incident response guidelines, checklists, and recommended procedures distributed to constituents to encourage consistency in response methods/standards?</td><td colspan="2">Priority II</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ Current incident response guidelines, checklists, and recommended procedures consistent with federal/organization requirements are maintained and provided to constituents.</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ There is limited distribution of incident response guidelines, checklists, and recommended procedures on a random basis.</td></tr>
<tr><td colspan="7">Prerequisites
❑ None
Control
❑ Documented procedures for distribution of procedures, guidelines, and checklists to constituency exist [R]
Activity
❑ Routine and as needed review and update of response guidelines [R]
❑ Immediate distribution of updated procedures to constituency [R]
Supporting Mechanisms
❑ Availability of information to constituents through multiple means (web, email, newsletter, manuals, awareness and training classes, etc.)
Artifacts
❑ Sample procedures, guidelines, and checklists, such as recovery procedures [R]
Quality
❑ Constituency understands how to use the guidelines, checklists, and procedures and are aware of their responsibilities for using them
❑ Constituent use of guidelines, checklists, and procedures is verified [R]
❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
<tr><td colspan="7">Regulatory References: None</td></tr>
<tr><td colspan="7">Guidance References: None
[indirect]
NIST SP 800-61 Computer Security Incident Handling Guide [Grance 2004]
Sec 3.3.4 Eradication and Recovery
[p 3-22] “Many valuable resources are available on the Internet for recovering and securing systems.”
[footnote 62] “http://csrc.nist.gov/publications/nistpubs/ provides links to the NIST Special Publications on computer security. CERT/CC also provides useful documents on securing systems and recovering from incidents at http://www.cert.org/tech_tips/.”</td></tr>
<tr><td colspan="7">Internal Organization References:</td></tr>
</table>

3.2.6 Are trusted relationships maintained with internal organizational experts who can give technical and non-technical advice and information?

This function focuses on the trusted relationships between those performing incident management activities and other experts or contacts within the organization who can provide assistance not only with technical aspects of incident management but also with non-technical aspects, such as public relations, legal issues, and human resources issues. This is a subjective question, but an important one. Incident management personnel without trusted contacts are isolated and may be in trouble in times of need.

Not applicable – To have this function be Not Applicable, incident management personnel would have to be positive they have all of the expertise they will ever need. This can be achieved in some strongly organized, distributed teams that are activated only when needed, in the unlikely case that they have achieved excellent planning and done a spectacular job of identifying all the experts, making them ad hoc or distributed members, training them on how to work as an ad hoc team, and keeping their membership information up to date. Selecting Not Applicable for this function must be accompanied by documented rationale. Again, the evaluator should use careful judgment to determine if this function is truly not applicable.

Impact statement – An incident management staff will be better positioned to quickly respond to situations that arise if it can 1) securely and effectively coordinate, collaborate, and exchange information with internal experts on a regular basis without error or misunderstanding and 2) call upon knowledgeable and trusted "gurus" for added expertise.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that incident management personnel not only has contacts with internal experts, but also trusts them, and keeps their contact information current to ensure rapid connections when their assistance is required. Keep in mind the subjectivity of this question (and its companion question for external experts in Function Table 3.2.7). The evaluator will have to judge if the indicators are met. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all of the required [R] indicators have been met. This is, in particular, the place where the evaluator must judge whether there is sufficient evidence that this function is being performed. Depending upon the nature of "trust" within the organization, there may be none of these artifacts or different artifacts to assess.
  - Also note that "contacted or worked with all of the POCs" means specifically checking to see that there are no *untested* POCs (someone who may once have been trusted by a former incident management staff member but has never been contacted by the current incident management personnel) or that the POCs are not *referrals*, meaning another trusted expert passed the name along but that person has not yet been verified.
- The [Partial] grade for this question can be achieved if the organization has started building trusted relationships and has started on the required indicators (i.e., has some of the policies, procedures, training, mechanisms, and POCs) in place to create and sustain the relationships.

Improvements – Developing a matrix of skills, knowledge, and people with their contact information could be an improvement to the internal processes.

Incident Management Capability Metrics						
3.2.6	**Are trusted relationships maintained with internal organizational experts who can give technical and non-technical advice and information?**			**Priority IV**		
Not observed ❑	Not applicable ❑	Yes	▪ Trusted relationships with other organizational experts who can assist are maintained.	Y ❑	P ❑	N ❑
		Partial	▪ A list of internal experts is being compiled.			

Prerequisites
- ❑ None

Control
- ❑ Documented policy exists for working with organization experts, including representatives from human resources, public relations, legal department, etc. [R]
- ❑ Documented process exists for contacting and working with organization experts [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]

Activity
- ❑ Personnel are aware and knowledgeable of the POC list and have contacted and worked with expert POCs [R]

Supporting Mechanisms
- ❑ Mechanisms to continue to develop trusted relationships (meetings, working groups, technical exchanges, MOU/SLAs, etc.) [R]

Artifacts
- ❑ Up-to-date POC list for trusted organization experts with phone numbers, email addresses, and other contact information [R]
- ❑ Minutes, records, actions, etc. of joint meetings, attendance at conferences or meetings, information exchanges
- ❑ MOU/MOA/SLAs with organization experts that define nature of the relationship and responsibilities

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References:
NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 2.4.4 Dependencies Within Organizations
[p 2-13] "It is important to identify other groups within the organization that may be needed to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including— […] Management […] Information Security […] Telecommunications […] IT Support […] Legal Department […] Public Affairs and Media Relations […] Human Resources […] Business Continuity Planning […] Physical Security and Facilities Management […]"

Internal Organization References:

3.2.7 Have trusted relationships been developed with other external experts (CERT/CC, FIRST, vendors, other entities, etc.)?

This function focuses on the trusted relationships between incident management personnel and external experts. Incident management personnel must establish and maintain trusted relationships with other experts who can provide assistance and information when needed. Trust takes time and effort to build and keep. It is not just a matter of having a name and phone number; personnel must be sure they can trust the information provided by the contact, and that contact must reciprocate that trust. This is a subjective question, but nonetheless, an important one. Incident management personnel with no one they can trust and turn to for assistance are isolated and may be in trouble in times of need.

Not applicable – It would not be advisable to not have contact points with other trusted organizations. Incident management personnel should have contacts with vendors and others external to the organization that it can call on when needed (for product support for vendor applications, anti-virus software, operating system vulnerabilities, etc.). There is no time during fast-moving incidents to try and work through approved channels to locate experts, have questions reviewed and approved, and wait for answers. If a CSIRT uses an intermediate person or group to gain access to external expertise, this metric will apply to that intermediary.

Impact statement – The incident management personnel can securely and effectively coordinate, collaborate, and exchange information with external experts on a regular basis without error or misunderstanding.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that incident management personnel not only have contacts with other external experts, but also trust them and maintain contact information to ensure rapid connections when assistance is required. Note this metric has a higher priority than the metric for trusted, internal experts because of the sensitivity of working with contacts outside the organization. Keep in mind the subjectivity of this metric (and its companion for internal experts in Function Table 3.2.6). The evaluator will have to use judgment to determine if the indicators are met. Specifically, the scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all of the required [R] indicators have been met. Note that there are no required artifacts. This is, in particular, the place where the evaluator must judge whether or not there is sufficient evidence that this function is being performed. Depending upon the nature of "trust" with external contacts, there may be none of these artifacts or different artifacts to assess.
  - Also note that "contacted all of the POCs" means specifically checking to see that there are no *untested* POCs (someone who may once have been trusted by a former incident management staff member but has never been contacted by the current staff) or that the POCs are not *referrals*, meaning another trusted expert passed the name along but that person has not yet been verified.
- The [Partial] grade for this question can be achieved if the organization has started building trusted relationships and has started putting the required indicators (i.e., has some of the policies, procedures, training, mechanisms, and POCs) into place to create and sustain the relationships.

Improvements – Establishing formal relationships with non-disclosure agreements is an improvement that can pave the way for very frank and open communications. Such relationships will expand the base of experts that can be called upon to assist with analysis, correlation, guidance, and other useful information that the IMC needs.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>3.2.7</td><td colspan="4">Have trusted relationships been developed with other external experts (CERT/CC, FIRST, vendors, other entities, etc.)?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ The team has established trusted relationships with other experts (CERT/CC, FIRST, vendors, other entities, etc.).</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ The team has identified experts and has begun establishing trusted relationships.</td></tr>
<tr><td colspan="7">Prerequisites
❑ None
Control
❑ Documented policy for working with external groups and experts exists [R]
❑ Documented procedures exist for vetting new contacts, establishing trust, and working with external experts
❑ MOU/MOA/SLAs or some other documentation exists between both that define the nature of the relationships and the responsibilities [R]
❑ Personnel are appropriately trained in the procedures for vetting new relationships
Activity
❑ Personnel have contacted all of the external experts and are familiar with those experts [R]
Supporting Mechanisms
❑ Up-to-date POC list for trusted technical experts with phone numbers, email addresses, and other contact information [R]
❑ Mechanisms to continue to develop trusted relationships (meetings, working groups, technical exchanges, conferences, etc.) [R]
❑ List of contacts with whom trusted relationships need to be established or re-established
Artifacts
❑ Minutes, records, actions, etc. of joint meetings, attendance at conferences or meetings, information exchanges
❑ Observation of personnel establishing or working with trusted contact (e.g., exchanging PGP/GnuPG keys with contact or vetting a new contact)
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures [R]
❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
<tr><td colspan="7">Regulatory References: None
[indirect]
FISMA Sec 3544(b)(7)(B) [OLRC 2003]
3544 “(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
‘‘(7) procedures for detecting, reporting, and responding to security incidents […] including— […]
‘‘(B) notifying and consulting with the Federal information security incident center referred to in section 3546 [US-CERT]”</td></tr>
</table>

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.3.2.4 Other Outside Parties [p 2-7, 2-8] "[…] an organization may want to discuss incidents with several other groups, including— The Organization's ISP […] Software Vendors […] Other Incident Response Teams […] It is highly recommended that the incident response team discuss with its public affairs office and legal department the circumstances under which each type of external organization can be contacted and the kind of information that can be provided. These procedures should be written, and all incident response team members should follow them."
Internal Organization References:

3.3 Incident Analysis

3.3.1 Is incident analysis conducted?

This function focuses on whether the organization analyzes all available information and supporting evidence or artifacts related to computer security events and incidents to determine the extent of damage and the impact on business functions. The purpose of the analysis is to identify the scope of the incident, nature of the incident, involved parties, timeframe, relationship of the incident to other activity, and available response strategies or workarounds. Incident management personnel may use the results of vulnerability and artifact analysis to understand and provide the most complete and up-to-date analysis of what has happened on a specific system.

Not applicable – Since this is a core function of any incident management capability, this function will always be applicable to someone or some group in the organization, even if it is not a CSIRT. Without performing this function there would be no way to understand the scale, effect, and potential threat of malicious or suspicious activity or incidents within the constituent enterprise infrastructure. A CSIRT usually takes the lead in performing incident analysis, but it is possible that analysis is done by others in the organization with specific skills and expertise. This question should also be applied to other groups that might perform this function.

Impact statement – Incident analysis is the key to determining what potential threats and malicious activity are actually dangers to the organization infrastructure. Timely analysis and resulting report dissemination will alert organization stakeholders to the proper response to be taken to protect key assets and data.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization not only understands the requirements and methodologies for performing incident analysis, but that the analysis is performed in a consistent, accurate, timely, and complete manner. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer for this question can be achieved only if all of the required indicators [R] are met.
- All other combinations of indicators yield a [No] answer.

Improvement – There are multiple indicators in the supporting mechanisms and quality areas that identify areas for improvement. Most deal with using appropriate tools and automated analysis techniques to ensure the analysis occurs as quickly and accurately as possible. Being able to track information and analysis in a tracking system or database allows for easier correlation and searching of related events, intruder MOs, exploits, and countermeasures.

Feedback from constituents can be used to highlight areas where changes must be made to improve the process. The indictor “The percentage of recommended countermeasures or improvements that are implemented can be verified” although not required, is the ultimate evaluation of the success of this function. If countermeasures and improvements are not being made, then there is an underlying problem that must be addressed to ensure the enterprise infrastructure is adequately protected.

Incident Management Capability Metrics				
3.3 Incident Analysis				
3.3.1	**Is incident analysis conducted?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Incident analysis is conducted on incidents.	Yes ❑	No ❑

Prerequisites

- ❑ Defined criteria for when analyses should be conducted on incidents exists [R]

Control

- ❑ Documented incident analysis policy and procedures exist [R]
- ❑ If performed, artifact analysis procedures stipulate the type and depth of analysis of artifacts (IDS logs, audit logs, system logs, malicious code, root kits, etc.) associated with incident(s) [R]
- ❑ Personnel are appropriately trained on the procedures, relevant technology, and relevant methodologies [R]

Activity

- ❑ Personnel conduct a level and type of analysis appropriate to the category and severity of incident [R]
- ❑ Incident analysis reports are generated according to the procedures and archived [R]
- ❑ Incident analysis reports are provided to affected constituents, and, as appropriate, sanitized information is provided to other constituents or external contacts as appropriate [R]

Supporting Mechanisms

- ❑ Tools supporting analysis of incidents [R]
- ❑ Incident tracking systems [R]
- ❑ Artifact analysis tools and methodologies
- ❑ Vulnerability analysis tools and methodologies

Artifacts

- ❑ Sample incident reports from constituents [R]
- ❑ Sample incident and other types of analysis reports [R]
- ❑ Sample recommendations for improvements or countermeasures [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, technologies, and methodologies used to perform this task [R]
- ❑ Analysis reports provide recommendations/countermeasures that feed into security improvement methods for incident management personnel and constituent system administrators/owners [R]
- ❑ There is a process and criteria (such as clarity, usefulness, applicability, and meaningfulness) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ❑ The percentage of recommended countermeasures or improvements that are implemented can be verified

Regulatory References: None

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.4 Incident Analysis [p 3-9] "[,,,] each indication should be evaluated to determine if it is legitimate." [p 3-10] "Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened. […] The incident response team should work quickly to analyze and validate each incident, documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. When in doubt, incident handlers should assume the worst until additional analysis indicates otherwise." [indirect] Sec 3.2.5 Incident Documentation
Internal Organization References:

3.3.2 Is fusion analysis (analyzing data from disparate sources) to identify concerted attacks and shared vulnerabilities performed?

Attacks and other malicious activity do not often occur in isolation. To identify the true scope of an incident, impact of a vulnerability, or risk of a potential threat, many different variables must be reviewed and analyzed. This type of analysis is referred to as fusion analysis. The result of such analysis is a big-picture view of security threats within, across, and external to a site. To perform fusion analysis, an organization must look at many different, disparate data sources. These sources can include research on well-known attacks, incident reports, vulnerability exposures, network traffic, system and network configurations and environments, media reports, and other situational awareness data. Through examination of such variables from multiple sites and sources, a concerted attack signature can be recognized, common widespread vulnerabilities can be identified, and potential victims of targeted attacks may be predicted. Based on this information, a better understanding of the full scope and impact of malicious activity and existing vulnerabilities can be determined.

Not applicable – This is a higher level form of research, requiring access to multiple data sources and requiring specific expertise for performing the analysis. Not all organizations may have the expertise or tools to perform it. Not performing such analysis can limit the full understanding of ongoing risks and threats and could result in ineffective countermeasures and recommendations. If this type of analysis is not done by the organization then this function can be marked as "Not Applicable."

Impact statement – Fusion analysis allows a better understanding of the relationship between ongoing incidents or potential threats that can result in the identification of more effective countermeasures and remediation strategies, providing a more widespread solution to computer security problems. With this understanding, more targeted and comprehensive recommendations and countermeasures for security improvements and countermeasures can be made.

Scoring and interpretation guidance – The goal of this question is to show that the organization understands the requirements and methods for fusion analysis and that the analysis is performed in a consistent, accurate, timely, and complete manner. The function is satisfactorily performed when data from multiple disparate sources are analyzed to provide a comprehensive view of threats and risks. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - fusion analysis results are occasionally used to improve the security posture of constituent infrastructure network and systems OR
  - only a small set of data from a few sources are analyzed OR
  - the organization has informal procedures for completing this task AND
    - personnel understand and follow the informal procedures consistently AND
    - recommendations for security improvements are given

Improvement – There are multiple indicators in the quality areas that identify areas for improvement. Most of these indicators deal with gathering feedback to determine how well the organization is performing this function and how effectively recommended solutions are applied. Gathering such data can help identify areas for improvement and better constituent satisfaction.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>3.3.2</td><td colspan="4">Is fusion analysis (analyzing data from disparate sources) to identify concerted attacks and shared vulnerabilities performed?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ Fusion analysis of data from disparate sources is performed to determine connections between attacks, vulnerabilities, threats, and weaknesses, and to provide constituents with recommendations for increased or improved security.</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ Data from only a few sources are analyzed. The analysis is not comprehensive but recommendations for improved security are given.</td></tr>
<tr><td colspan="7">Prerequisites
❑ Various sources of data, incidents, and vulnerabilities are available and accessible [R]
Control
❑ Documented fusion analysis policy and procedures exist [R]
❑ Personnel are appropriately trained on the procedures, relevant technology, and methodologies [R]
Activity
❑ Data from disparate sources is routinely synthesized to determine connections between events, incidents, and vulnerabilities, providing an enterprise view of threats and attacks (fusion analysis) [R]
❑ Fusion analysis reports are generated according to the procedures and archived [R]
❑ Fusion analysis reports are provided to appropriate technical and management personnel; sanitized information is provided to other external contacts as appropriate [R]
❑ Analysis reports provide recommendations/countermeasures that feed into security improvement methods for incident management personnel and constituent system administrators/owners [R]
Supporting Mechanisms
❑ Tools supporting fusion analysis [R]
❑ Incident data/information tracking system [R]
Artifacts
❑ Samples of reviewed data (incident reports, vulnerability reports, system and network configurations, network traffic logs, etc.) [R]
❑ Sample fusion analysis reports identifying common problems, related attacks and shared vulnerabilities [R]
❑ Sample recommendations for improvements or countermeasures [R]
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, technologies, and methodologies used to perform this task [R]
❑ There is a process and criteria (such as timeliness, completeness, clarity, usefulness, applicability and accuracy) for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
❑ The percentage of recommended countermeasures or improvements that are implemented can be verified</td></tr>
<tr><td colspan="7">Regulatory References: None</td></tr>
</table>

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.3 Sources of Precursors and Indications [p 3-7] "Precursors and indications are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people." Sec 3.2.4 Incident Analysis [p 3-11] "Perform Event Correlation. Evidence of an incident may be captured in several logs. […] Correlating events among multiple indication sources can be invaluable in validating whether a particular incident occurred, as well as rapidly consolidating the pieces of data."
Internal Organization References:

3.3.3 Is retrospective analysis conducted?

This function focuses on whether information and reports are analyzed from a historical perspective to provide both a comprehensive view of emerging threats and risks and an evaluation of the success of resolution strategies. Retrospective analysis can look at the actions that have been taken to manage incidents, attacks, and vulnerabilities over time and compare them to the current state to determine if those actions had positive long-term effects or successful outcomes (i.e., those problems are not recurring and were successfully mitigated). Such analysis requires looking at response times, response strategies, changes in reports over time, and changes in the security posture of the organization. The types of incidents, vulnerabilities, and attacks that have been seen overtime are also reviewed. In this case, the analysis is used to help identify high-risk areas, continuing and high-volume incidents, and emerging problem areas.

Not applicable – This is a higher level analysis, requiring access to historical data about incidents, attacks, vulnerabilities, actions taken, and changes in the infrastructure or environment. Performing this task can require specific skills and expertise. Not all organizations may have the expertise, historical data, or time to perform such analysis. If doing this type of analysis is not in the organization's mission then this function can be marked as "Not Applicable."

Impact statement – Retrospective analysis identifies ineffective resolutions that require new solutions or identifies emerging problem areas that require attention. This will provide for a better overall computer security strategy plan and implementation. It also can confirm positive actions that have strengthened the organization's ability to correct security problems.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization not only understands the requirements and methodologies for performing retrospective analysis, but that the analysis is performed in a consistent, accurate, timely, and complete manner. The question is satisfied when the organization analyzes historical data to determine how effective resolution strategies have been and to identify areas for further improvement. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - retrospective analysis is only occasionally performed OR
  - retrospective analysis results are occasionally used to improve the security posture of constituent infrastructure network and systems OR
  - the organization has informal procedures for completing this task AND
  - personnel understand and follow the informal procedures consistently

Improvement – There are multiple indicators in the quality areas which identify areas for improvement. Most deal with using gathered feedback to determine how well the organization is performing this function and how effectively recommended solutions are applied. Gathering such data can help identify areas for improvement to better meet constituent expectations and identify needs such as for new tools or additional training.

Incident Management Capability Metrics						
3.3.3	**Is retrospective analysis conducted?**					**Priority IV**
Not observed ❑	Not applicable ❑	Yes	▪ Retrospective analysis is routinely conducted.	Y ❑	P ❑	N ❑
		Partial	▪ Retrospective analysis is occasionally conducted.			

Prerequisites

- ❑ Historical data on incidents, vulnerabilities, and applied countermeasures is available and accessible [R]

Control

- ❑ Documented retrospective analysis policy and procedures exist [R]
- ❑ Personnel are appropriately trained on the procedures, relevant technology, and methodologies [R]

Activity

- ❑ Historical data and information related to incidents, attacks, vulnerabilities, and applied countermeasures are routinely reviewed to determine long-term effects, outcomes, emerging problems, and trends [R]
- ❑ Retrospective analysis reports are generated according to the procedures and archived [R]
- ❑ Retrospective analysis reports are provided to appropriate technical and management personnel, sanitized information is provided to other external contacts as appropriate [R]
- ❑ Analysis reports provide recommendations/countermeasures that feed into security improvement methods for incident management personnel and constituent system administrators/owners

Supporting Mechanisms

- ❑ Tools supporting retrospective analysis [R]
- ❑ Incident management worklogs
- ❑ Incident tracking systems or databases or access to reports/data [R]
- ❑ Vulnerability databases[R]

Artifacts

- ❑ Samples of reviewed data (e.g., incident reports, vulnerability reports, worklogs, recommendations, and reports on countermeasures taken, etc.) [R]
- ❑ Sample retrospective analysis reports [R]
- ❑ Sample recommendations for improvements or countermeasures

Quality

- ❑ Defined quality criteria including what is timely, complete, and accurate exist [R]
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, technologies, and methods used to perform this task [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness (including the of percentage of recommended countermeasures or improvements that are implemented) of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]

Sec 3.4.2 Using Collected Incident Data

[p 3-23] "Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. […] A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team. […]"

Incident Management Capability Metrics
Internal Organization References:

3.3.4 Is incident correlation performed?

This function focuses on whether activity across incidents is correlated to determine any interrelations, patterns, common intruder signatures, common targets, or common vulnerabilities being exploited. Types of information that may be correlated include: IP addresses, hostnames, ports, protocols, services, applications and operating systems, organizational sectors, site names, and business functions. Such analysis will broaden the picture of the scope and nature of the activity, identifying where activity is more widespread than originally thought and identifying relationships between malicious attacks and compromises and exploited vulnerabilities. Based on the output of the correlation, additional analyses can be done to determine what patterns of attacks are emerging and what security problems must be addressed. With this information, organizations can determine effective resolution and mitigation strategies and have an idea of all points where they must be applied.

Not applicable – Correlation of incident data is a core task of any incident handling function. It would be unlikely that this function would not be performed. If this type of analysis is not done by the organization and the organization does not use the correlation and trend analysis done by others then this function can be marked as Not Applicable.

Impact statement – Incident correlation broadens the view of the nature and scope of malicious activity, identifying relationships and interdependencies that can be useful in developing and implementing comprehensive solutions, ensuring more effective and efficient security strategies.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization not only understands the requirements and methodologies for performing incident correlation and trend analysis, but that the analysis is performed in a consistent, accurate, timely, and complete manner. The question is satisfied when the organization analyzes incidents to determine interrelationships between them and emerging trends. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - incident correlation is performed in a limited fashion OR
  - the organization depends upon the incident correlation conducted by other organizations or vendors OR
  - the organization has informal procedures for completing this task AND
  - personnel understand and follow the informal procedures consistently

Improvement – There are multiple indicators in the quality areas that identify areas for improvement. Most deal with using gathered feedback to determine how well the organization is performing this function and how effectively recommended solutions are applied. Gathering such data can help identify areas for improvement to better meet constituent expectations and needs. Instituting automated correlation tools in any incident tracking or logging systems may be one improvement that organizations should strive to make. Such tools can decrease the time it takes to determine interrelationships between incidents. Incidents viewed in isolation may not seem to be connected. The faster these connections are identified, the better comprehensive understanding of ongoing activity and needed response strategies will be. This will result in the implementation of better mitigation and resolution strategies.

Incident Management Capability Metrics						
3.3.4	**Is incident correlation performed?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ Incident correlation is performed.	Y ❑	P ❑	N ❑
		Partial	▪ There is limited ability to perform incident correlation. OR ▪ Intermittent use of generic incident correlation is conducted by other organizations or vendors.			

Prerequisites
- ❑ Archive of event/incident information to support correlation exists [R]
- ❑ Access to other organizations for incident correlation information, if required or possible [R]

Control
- ❑ Documented correlation policy and procedures exist [R]
- ❑ Personnel are appropriately trained on the procedures, relevant technology, and relevant methodologies for performing this type of analysis [R]

Activity
- ❑ Incident correlation is conducted, or information is obtained and analysis reports are developed [R]
- ❑ Recommendations are developed, as appropriate, based on correlation analysis
- ❑ Personnel know how to obtain and use analysis reports provided by other organizations or vendors.
- ❑ Analysis reports are generated according to the procedures and archived
- ❑ Incident correlation reports are provided to appropriate technical and management personnel, sanitized information is provided to other constituents if applicable [R]

Supporting Mechanisms
- ❑ Correlation and trend analysis tools and methodologies [R]
- ❑ Incident tracking system or database

Artifacts
- ❑ Samples of incident reports
- ❑ Samples of correlation and trend analysis reports [R]
- ❑ Sample recommendations for improvements or countermeasures

Quality
- ❑ Personnel are aware and knowledgeable of the procedures, technologies, and methodologies used to perform this task [R]
- ❑ Personnel consistently follow the procedures [R]
- ❑ Periodic reviews of analysis reports for clarity, usefulness, applicability, and meaningful results are conducted
- ❑ Analysis reports provide recommendations/countermeasures that feed into security improvement methods for incident management personnel and constituent system administrators/owners
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ❑ The % of recommended countermeasures or improvements that are implemented can be verified
- ❑ Automated correlation tools are built into any incident tracking or logging system

Regulatory References: None

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.3 Sources of Precursors and Indications [p 3-7] "Precursors and indications are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people." Sec 3.2.4 Incident Analysis [p 3-11] "Perform Event Correlation. Evidence of an incident may be captured in several logs. […] Correlating events among multiple indication sources can be invaluable in validating whether a particular incident occurred, as well as rapidly consolidating the pieces of data."
Internal Organization References:

3.3.5 Is forensics analysis performed on constituent systems and networks?

This function focuses on whether the organization performs the collection, preservation, documentation, and analysis of evidence from a compromised computer system to identify changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; looking for the remains of files in dynamic memory or swap and cache areas; and checking for Trojan horse programs and toolkits.

Policies and procedures in place must assure that incident management personnel are knowledgeable and trained on using analysis tools and capturing forensics evidence so as not to damage or invalidate the data. These policies and procedures should also outline how and when law enforcement is involved in the analysis. Personnel performing this function may also have to be prepared to act as expert witnesses in court proceedings if the evidence analyzed is used in a court of law to prosecute the intruder.

Not applicable – This is a very specialized form of analysis, requiring special tools, training, skills, and processes. An organization may not have the expertise or resources to perform such analysis. Where this is the case, and the organization does not engage an outside party to perform this function, the function can be marked as Not Applicable.

Impact statement – Forensic analysis can be used to determine the nature and extent to which a system or network has been compromised or otherwise affected. This results in a better understanding of what malicious activity occurred and what other systems or services may have been affected. Such analysis can also facilitate development and implementing of comprehensive solutions, ensuring that more effective protective strategies are put in place. This information can also be used to prosecute malicious intruders.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization not only understands the requirements and methodologies for performing forensic analysis, but that the analysis is performed in a consistent, accurate, timely, secure, and complete manner that follows the chain of custody rules. The question is satisfied when systems and networks are analyzed to determine the exact changes that have been made and when the analysis is documented according to the rules of evidence. The scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required [R] indicators are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - forensic analysis is performed in a limited or ad hoc fashion OR
  - the organization depends upon the forensic analysis conducted by other organizations such as third-party experts, vendors, or law enforcement

Improvement – There are multiple indicators that identify areas for improvement. Following processes and procedures for collecting data in a forensically sound manner and conducting

analyses using similar approaches can improve how effective the incident management personnel will be in conducting response actions. (See Impact statement section above.)

Incident Management Capability Metrics						
3.3.5	**Is forensics analysis performed on constituent systems and networks?**			**Priority IV**		
Not observed ❑	Not applicable ❑	Yes	▪ Forensics analysis is conducted on constituent systems or networks as required.	Y ❑	P ❑	N ❑
		Partial	▪ Forensics analysis is conducted in an ad hoc or inconsistent manner. OR ▪ The organization depends upon the forensics analysis conducted by other organizations such as third-party experts, vendors, or law enforcement.			

Prerequisites

- ❑ There is an identified point of contact for working with law enforcement
- ❑ There are defined criteria for when and how law enforcement should be contacted.
- ❑ There are defined criteria for when forensics analyses should be conducted on incidents [R]

Control

- ❑ Documented forensics analysis policy and procedures exist [R]
- ❑ Procedures for following chain-of-custody and rules of evidence exist [R]
- ❑ Personnel are appropriately trained on the procedures, relevant technology, and methodologies [R]

Activity

- ❑ Forensics evidence is collected and analyzed [R]
- ❑ Forensics analysis reports are generated according to the procedures and archived [R]
- ❑ Forensics analysis results or reports are provided to appropriate technical, management, and legal personnel, sanitized information is provided to other constituents if applicable [R]
- ❑ Forensic evidence and analysis is passed to law enforcement for prosecution when appropriate and approved
- ❑ Analysis reports provide recommendations/countermeasures based on forensics analysis

Supporting Mechanisms

- ❑ Forensics analysis tools and techniques [R]
- ❑ Safes and other secure storage areas for evidence [R]

Artifacts

- ❑ Forensic analysis results or reports [R]
- ❑ Documentation showing chain of evidence [R]
- ❑ Sample recommendations for improvements or countermeasures
- ❑ Toolkit of system examination programs, file integrity checkers, etc.

Quality

- ❑ Personnel are aware and knowledgeable of the procedures, technologies, and methodologies used to perform this type of analysis [R]
- ❑ Personnel consistently follow the procedures [R]
- ❑ Analysis reports provide recommendations/countermeasures that feed into security improvement methods for incident management personnel and constituent system administrators/owners
- ❑ There is a process and criteria (such as clarity, usefulness, applicability, and meaningfulness) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness (such as preservation of the chain of evidence and the number of recommended countermeasures or improvements that are implemented) of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: None [indirect] (retain incident handling records for at least three years) General Records Schedule 24 - *Information Technology Operations and Management* Records [NARA 2003] 7. Computer Security Incident Handling, Reporting and Follow-up Records. "Destroy/delete 3 years after all necessary follow-up actions have been completed."
Guidance References: None NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec. 3.3.2 Evidence Gathering and Handling [p 3-18] "Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies, so that it should be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence […]" Sec 3.4.3 Evidence Retention [p 3-25] "**Prosecution**. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished. **Data Retention**. Most organizations have data retention policies that state how long certain types of data may be kept. […] General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years."
Internal Organization References:

3.3.6 Do the analytical processes incorporate methods to determine the risk or threat level of a confirmed incident?

This function focuses on whether incident management personnel are able to determine, with a reasonable degree of accuracy and consistency, the level of threat or risk to the constituent systems posed by an incident. Without the ability to do this, the organization will not know if the incident is significant or be able to judge the required speed and extent of the necessary response. Being able to assess the threat or risk requires some knowledge of what systems and information are important and the defined levels of threat and risk used by the organization.

The prerequisite states that incident management personnel must have current documentation on constituent systems criticality and the assets on those systems. Without this information, risk or threat can only be evaluated abstractly.

Not applicable – It would be imprudent to not have this capability built into any CSIRT or incident management capability. Without a risk or threat assessment, potential damage and impact to business systems, data, and operations cannot be determined and the appropriate response at the right level of urgency will not occur. There should not be a situation where an organization does not perform this function.

Impact statement – Performing risk or threat assessment and analysis provides insight into the overall impact that malicious activity can cause to business systems, data, and operations. This will provide direction in responding to the most critical incidents in the most effective and efficient way possible.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to show that the organization incorporates a consistent methodology for assessing the threat and risk of a confirmed incident into any analysis performed. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer can be achieved only if all of the required [R] indicators are met.
- All other combinations of indicators yield a [No] answer.

Improvement – There are multiple indicators in the control and quality areas that identify areas for improvement. Using gathered feedback to determine how well the organization is performing this function can help identify areas for improvement to better meet constituent expectations and needs.

Incident Management Capability Metrics				
3.3.6	**Do the analytical processes incorporate methods to determine the risk or threat level of a confirmed incident?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ The analytical processes incorporate methods to determine the threat, risk, or damage an incident may impose on constituent networks.	Y ❑	N ❑

Prerequisites

- ❑ Inventory of constituent critical systems, services, and data is available [R]
- ❑ Defined levels of risk or threat and associated levels of impact (damage) for the organization (including or accounting for business/mission risk) exist and are available [R]

Control

- ❑ Criteria for evaluating incident severity relative to constituent assets, data, and services and business operations exist [R]
- ❑ Processes and procedures to identify specific risks/threats to constituent networks exist [R]
- ❑ Personnel are appropriately trained on the procedures, relevant technology, and methodologies for performing this task [R]
- ❑ Current documentation of constituent system and network components is available

Activity

- ❑ Incident management personnel receive incident or vulnerability reports [R]
- ❑ Incident management personnel evaluate malicious activity propagation (or chance of such propagation occurring) through constituent networks [R]
- ❑ Incident management personnel evaluate levels of risk or threat and associated levels of impact (damage) for confirmed incidents and vulnerabilities and use this to help determine priority and type of response [R]
- ❑ Incident management personnel provide risk/threat analysis reports to appropriate technical and management, personnel and to constituents whose systems are at risk [R]

Supporting Mechanisms

- ❑ Incident tracking systems or databases
- ❑ Risk or threat analysis tools and methodologies [R]

Artifacts

- ❑ Sample incident reports
- ❑ Sample Incident risk or threat assessments or reports [R]

Quality

- ❑ Personnel conducting this analysis have a thorough knowledge of constituent networks to determine level of risk posed by incident/threat
- ❑ Personnel are aware of, knowledgeable of, and consistently follow these procedures and have the needed skills and analysis abilities [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness (e.g., completeness, accuracy, clarity, usefulness, and adherence to defined levels of risk/threat/impact) of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(7)(A) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]

''(7) procedures for detecting, reporting, and responding to security incidents […] including

''(A) mitigating risks associated with such incidents before substantial damage is done"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.2.4 Incident Analysis [p 3-10] "The incident response team should work quickly to analyze and validate each incident, documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. When in doubt, incident handlers should assume the worst until additional analysis indicates otherwise." Sec 3.2.6 Incident Prioritization [p 3-14, 3-15] "Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on two factors: Current and Potential Technical Effect of the Incident. […] Criticality of the Affected Resources. […] Organizations should document prioritization guidelines in a format such as the sample matrix shown in Table 3-4. […] Organizations should customize the matrix based on their own needs and their approach to identifying resource criticality"
Internal Organization References:

SUSTAIN: SECTION 4 OF INCIDENT MANAGEMENT CAPABILITY METRICS

This process focuses on the ability of the organization to identify and implement what needs to be in place for incident management to occur in a timely and effective manner. For this to occur, there must be a defined incident management mission with supporting goals and objectives, well-defined policies and procedures, skilled staff, service definitions, technological resources, and other processes and equipment to promote the function. Also required are the supporting infrastructure, controls, supporting mechanisms, artifacts, and quality measures that enable incident management to perform its functions. In this regard, it has appropriate contracts, MOUs, and SLAs established that define roles and responsibilities, financial planning and budgeting processes to sustain operations over time, training and educational opportunities for staff, program management plans, and more.

Part of any sustainment function includes improving the overall effectiveness of the operations. This is also true in the case of a CSIRT or incident management capability. As events and incidents are handled and response is provided, any lessons learned should be captured and fed into process improvements. Additionally, any results from risk assessments or vulnerability scanning activities can also be reviewed to determine any changes needed in processes, technology, personnel skills, or other areas.

The Sustain metrics include subcategories in the following areas:

- **MOU** (Memorandum of Understanding), MOA (Memorandum of Agreement), LOA (Letter of Agreement), SLA (Service Level Agreement), and Contracts – to formalize activities and define services provided by the CSIRT and to establish correct expectations for operations
- **Project/Program Management** – to provide guidance and oversight for continued incident management operations, financial planning, business resumption, and other relevant activities
- **CND Technology Development, Evaluation and Implementation** – looks at the ability of the organization to test software and analyze impacts prior to implementing in production networks; examines new technologies that are incorporated into the infrastructure
- **Personnel** – focuses on ensuring there is a cadre of personnel with the required knowledge, skills, and abilities to perform the work and to continue to develop professionally in order to meet the changing needs of the constituency that it serves
- **Security Administration** – covering physical security measures and operations security
- **CND Information Systems** – ensures the organization utilizes a defense-in-depth approach for hardening systems and networks (data protection, monitoring, risk assessments, vulnerability scanning, patch management strategies, communications methods, etc.) used for incident management functions
- **Threat Level Implementation** – focuses on the organization's ability to maintain and adhere to threat levels and to assist consistently with threat level issues

4. Sustain

4.1 MOUs and Contracts

4.1.1 Is there an incident management function or CSIRT designated by the organization head or CIO through an official appointment order?

This function assesses whether a group(s) or a CSIRT has been established as the officially designated authority for incident management functions within the organization. This helps ensure senior executive support of the incident management mission, thereby helping the organization members to understand the CSIRT's (or groups') role and authority. Such a designation can be made through an official policy statement, an executive memo, or a simple announcement. Having only a procedure that lists the CSIRT is insufficient.

Not applicable – Clearly designating the roles and responsibilities for incident handling will improve the overall reaction time and effort for the organization. If a CSIRT is not formally or informally appointed or recognized by its constituency it will be difficult for it to operate in a consistent and effective fashion. Because of this, it is unlikely that this metric would not be applicable. Also, if the CSIRT is not designated, another area of the organization may be given this responsibility in which case it would be evaluated against this metric.

Impact statement – If this function is effectively performed, accountability and responsibility for incident management is clearly designated. This will reduce confusion over who is the appropriate person to act, reduce duplicate effort by assigning roles and answerability, and streamline the processes, ensuring the right people are involved in the right way.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is for all personnel within the organization to be fully cognizant of the roles and levels of authority associated with incident management, as established by the organization's senior executive management.

- The [Yes] answer for this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] score for this question can be achieved if
  - senior organization management considers the CSIRT or designated group to be the incident handling focal point AND
  - the designation of CSIRT/designated groups has not been formally established OR
  - the CSIRT/designated group generally acts as the organization's incident handling focal point OR
  - organization personnel generally consider the CSIRT or designated group to be the primary incident handling focal point
- The failing grade on this function results if the CSIRT or some other designated group is not in some way recognized as the focal point for organization IT security incidents.

Improvement – Improvements can be achieved by documenting this designation in an official written publication, memo, or policy and also by making this written designation easily accessible to the constituency. Other improvements could be achieved by building mechanisms for educating the constituency on the roles and responsibilities of incident management personnel. This might include adding such information and the corresponding appointment order or announcement to

orientation materials, incident reporting guidelines, employee handbooks, and other similar materials.

Incident Management Capability Metrics						
4. Sustain						
4.1 MOUs and Contracts						
4.1.1	**Is there an incident management function or CSIRT designated by the organization head or CIO through an official appointment order?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ The CSIRT has been officially designated by the organization as such in a formal order.	Y ❑	P ❑	N ❑
		Partial	▪ The CSIRT is informally recognized by the organization.			

Prerequisites
- ❑ None

Controls
- ❑ Executive support of incident management mission exists [R]

Activity
- ❑ An entity or specific person has been designated as the incident management "lead" [R]
- ❑ Policy or other official designation is documented and distributed or available throughout the organization

Supporting Mechanisms
- ❑ Policy dissemination, archive, and retrieval mechanism

Artifacts
- ❑ Organizational policy or other formal document designating the CSIRT or other group as the incident response provider [R]
- ❑ Written artifacts from organization executive management that informally designating the CSIRT or other group/person as the principal incident handling point of contact

Quality
- ❑ Personnel are aware of location of organization policy or formal declaration

Regulatory References: None
[indirect]
FISMA Sec 3544(a)(4) [OLRC 2003]
3544 "(a) IN GENERAL—The head of each agency shall …:
''(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Guidance References: None
[indirect]
NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 2.3.1 Policy and Procedure Elements
[p 2-3] "[…] most policies include […] organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents."

Internal Organization References:

4.1.2 Is there a documented agreement(s) that identifies the incident management services provided to the constituency?

This function focuses on ensuring that the organization clearly sets the expectations regarding what incident management services will be provided, to whom, by whom, the associated costs, and so on. Setting these expectations early helps avoid confusion and misunderstandings later.

Not applicable – This function should always be applicable since having a formal or informal agreement covers all cases. The agreement, either written or informal, should exist to ensure that the CSIRT or incident management personnel and the constituency know how to interact with one another.

Impact statement – If this function is effectively performed, the constituency understands clearly what assistance they can obtain from incident management personnel and what timeframes and operational procedures must be met. Such agreements manage expectations of both parties, reduce confusion, and delineate how interfaces should be maintained. All of this works to improve the general incident management capability of the organization.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to delineate resource availability for handling emergencies, as well as to set expectations of the service levels.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] score for this question can be achieved if
  - there are implied or informal agreements between the constituency and incident management personnel detailing services provided OR
  - there is a general consensus among the constituency of the incident management services provided AND
  - these services are consistently provided by incident management personnel
- The [No] answer on this question results when there are no written or even informal agreements with the constituency detailing the incident management services.

Improvement – Improvements can be achieved by documenting the range and level of incident management services provided to the constituency, along with operational timeframes and deliverables, in some type of service level agreement (SLA) or other written document. This agreement should also be easily accessible by the constituency and frequently updated if changes in service levels occur. Other improvements could be achieved by building mechanisms for educating the constituency on the incident management services. This might include building such information into orientation materials, incident reporting guidelines, employee handbooks, and other similar materials.

Incident Management Capability Metrics						
4.1.2	**Is there a documented agreement(s) that identifies the incident management services provided to the constituency?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ There is a documented agreement with the constituency that details the services provided.	Y ❑	P ❑	N ❑
		Partial	▪ There are undocumented, informal agreements with the constituency.			

Prerequisites

- ❑ A defined constituency exists [R]
- ❑ The incident management services to be provided are determined

Controls

- ❑ Services agreement is sufficiently detailed for a clear understanding of expectations, including the type, depth, and breadth of services provided to constituency (e.g., public web site, SLA, MOU, etc.) [R]

Activity

- ❑ Personnel work with the constituency to set and manage expectations of what services can and will be delivered
- ❑ Operational timeframes for notifications, support, etc., are determined and mutually agreed upon in advance [R]

Supporting Mechanisms

- ❑ Mechanism to inform constituents of services provided – e.g., web site, mailing list
- ❑ Mechanism for determining business critical elements on demand during incident operations
- ❑ Alerting channel or mechanism to inform constituency of activity

Artifacts

- ❑ Copy of written agreement (e.g., MOU, SLA, MOA, LOA) that has been signed by management or official web page or other document that clearly announces the agreed upon services [R]

Quality

- ❑ Constituents clearly understand what incident management services are provided to whom, when, etc.
- ❑ Agreement includes commitment by constituency to identify mission critical processes, servers, and other infrastructure elements
- ❑ Contract includes SLA specifying timelines for operational functions such as notification period, on-site assistance, support tier escalation, etc.
- ❑ Agreement specifies that the constituent will be notified of any incident management activities that may affect network operations
- ❑ If another service provider, contractor or organization provides incident management services, these arrangements are documented in the agreement with constituency

Regulatory References: None

Guidance References: None

[indirect]
NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 2.5 Incident Response Team Services
[p 2-14] "[…] it is fairly rare for a team to perform incident response only."
[footnote 26] "CERT/CC provides a more detailed list of potential team services at http://www.cert.org/csirts/services.html."
Sec 2.6 Recommendations
[p 2-16] "Determine which services the team should offer."

Internal Organization References:

4.1.3 Does the agreement with the constituent specify that the constituency will provide notification in advance of changes or planned outages to its network?

This function focuses on ensuring that incident management personnel are kept up to date about all constituent infrastructure changes. Without this information they may not be able to adequately assess the validity of a given event or incident report. Such notifications help them determine when reported behavior may have been caused by normal maintenance or configuration updates, rather than malicious intruder activity that disables part of the constituency network. This also facilitates an accurate inventory of system and network components.

Not applicable – This metric should always be applicable since having a formal or informal agreement covers all cases. The agreement, either written or informal, should exist to ensure that incident management personnel and the constituency know how to keep each other informed.

Impact statement – Through this notification incident management personnel are able to better assess the cause of any reported event or incident, decreasing the research and analysis time needed to determine the appropriate response. They are working with a full understanding of the infrastructure and can make better decisions regarding risk assessments, threat levels, and recovery strategies.

Scoring and interpretation guidance – The goal of satisfying this metric is tight configuration management of network assets and a full understanding of the status of critical systems and data.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] answer to this question can be achieved if
  - verbal agreements exist between the constituency and incident management personnel to provide this notification OR
  - there is an implied understanding that the constituency will provide this notification AND
  - notification is consistently provided by the constituency
- The [No] answer to this question is achieved if the majority or all of the required indicators [R] are not met.

Improvement – Improvements can be achieved by documenting, in writing, the policies, procedures, and processes for notifying incident management personnel of any constituent infrastructure changes or outages. These documents should also be easily accessible by authorized personnel in both the constituency and the incident management capability. Other improvements could be achieved by incorporating incident management personnel into any change management system and announcements. This incorporation would be best served if incident management personnel were also able to provide input and recommendation for desired configuration changes. An automated change management system or inventory would provide an efficient tool for archiving such infrastructure changes and allow them to be easily searched and reviewed.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>4.1.3</td><td colspan="4">Does the agreement with the constituent specify that the constituency will provide notification in advance of changes or planned outages to its network?</td><td colspan="2">Priority III</td></tr>
<tr><td rowspan="2">Not observed ❑</td><td rowspan="2">Not applicable ❑</td><td>Yes</td><td>▪ The agreement specifies that the constituency will provide notification of changes such as configuration changes, scheduled power outages, and maintenance on critical network assets.</td><td rowspan="2">Y ❑</td><td rowspan="2">P ❑</td><td rowspan="2">N ❑</td></tr>
<tr><td>Partial</td><td>▪ There is a verbal agreement or “understanding” with the constituents to provide this notification, but it is done correctly.</td></tr>
<tr><td colspan="7">Prerequisites
❑ Constituency maintains schedules and plans of network outages and changes [R]
❑ Constituency is responsible for making changes to the network [R]
Controls
❑ Agreement (e.g., MOU, MOA, LOA, SLA) stipulates what types of changes will be reported, along with notification timelines, such as [R]
- Notification to CSIRT or incident management personnel
- Constituent plans for minimum outage time
- Constituent plans for minimum impact to operations
- Constituent plans for continued operations in the event of maintenance failures (e.g., redundant or backup system(s))
❑ Period of advance warning is agreed to for normal situations
❑ Incident management personnel support during maintenance or extended outage is outlined
Activity
❑ Advance warning is given concerning network changes or outages [R]
Supporting Mechanisms
❑ Alerting channel or mechanisms for sending outage and change management reports [R]
❑ Change management systems
❑ Configuration management systems
Artifacts
❑ Agreement document
❑ Details of advance warning items, period, etc.
❑ Historic copies of prior warnings [R]
Quality
❑ Incident management personnel are aware and knowledgeable of the contents of the agreement [R]
❑ Constituent personnel are aware and knowledgeable of the contents of the agreement
❑ Notification occurs in compliance with agreement terms such as within the proper timeframe
❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
<tr><td colspan="7">Regulatory References: None</td></tr>
<tr><td colspan="7">Guidance References: None</td></tr>
<tr><td colspan="7">Internal Organization References:</td></tr>
</table>

4.2 Project/Program Management

4.2.1 Is there a financial plan for incident management functions?

This function focuses on the program management efforts in planning and budgeting for future incident management requirements. The incident management arena is highly dynamic, and to be as prepared as possible, the appropriate staff, equipment, and infrastructure must exist. This includes training for staff on new attack types, incident handling and security tools, and new methods and technologies for responding to events and incidents. Without a financial plan, an organization cannot ensure continued growth or even continued daily operations for incident management. Note that where some services or functions are provided by contractors or managed service providers, there may be additional financial plans addressing each contractor. These may have specific standards and guidelines. Also note that the incident management financial plan may be part of a larger financial plan; in that case, it is important that incident management personnel have some control over what is proposed and incorporated into that larger plan.

Not applicable – This function should always be applicable since some part of the organization performs budget planning. If the CSIRT or designated incident management personnel do not maintain this capability, the part of the organization that does should be evaluated as it applies to planning for incident management functions.

Impact statement – A comprehensive financial plan will ensure that incident management personnel can meet their current obligations while planning for expansion and growth, as appropriate.

Note that ad-hoc incident management teams may not have any financial plans. This can make it extremely difficult to get approval for increased budgets, allocation of equipment and needed resources, and the like.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is ensuring the continuing operational, incident management capability.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] answer to this question can be achieved if
  - the organization is in the process of developing a financial plan for incident management OR
  - incident management personnel have effective input into the financial planning for its operation, but that planning is managed by another part of the organization (can they really get what they need, when they need it)
- The [No] answer to this question is achieved if the majority or all of the required indicators [R] are not met.

Improvement – Improvements can be achieved by providing training for those incident management personnel responsible for financial planning of various techniques for developing and meeting long-term budgeting requirements. Other improvements can be made by ensuring that all plans are in compliance with organization and other regulatory requirements. Financial plans and budgets should include funds for sustaining the overall quality of the incident management capability. To enable staff to keep pace with the changes in technology and usage,

there should be an ongoing budgeting plan for continuing education or refresher courses so that incident management personnel can continue to be effective incident handlers. In addition, where appropriate, budget plans should also include funds to provide opportunities for professional development to further enhance the team members' knowledge and abilities, keep them engaged and energized about incident management work, expand the overall capabilities of the team, and possibly to meet any requirements for certifications that may be required for certain incident management personnel.

Incident Management Capability Metrics						
4.2 Project/Program Management						
4.2.1	**Is there a financial plan for incident management functions?**			**Priority IV**		
Not observed ❑	Not applicable ❑	Yes	▪ There is a financial plan in compliance with regulatory requirements.	Y ❑	P ❑	N ❑
		Partial	▪ A financial plan is currently being developed.			

Prerequisites
- ❑ Organization conducts annual budget planning cycle

Controls
- ❑ Incident management personnel or managers determine, recommend, and control (to the extent possible) the future budgetary requirements [R]

Activity
- ❑ Budget projection estimates are periodically conducted [R]
- ❑ N-year financial and infrastructure plan is built [R]
- ❑ The financial plan is periodically reviewed and updated (due to newly discovered needs in equipment, personnel, policy, procedure, etc.)
- ❑ Personnel are trained in financial planning and budgeting techniques and methodologies
- ❑ Personnel are trained in financial plan compliance regulations applicable to their organization [R]

Supporting Mechanisms
- ❑ Organization budgeting process, spreadsheets, and/or other supporting tools

Artifacts
- ❑ Financial plan documentation [R], including
  - identified staffing
  - equipment
  - supporting costs
- ❑ Contractor or other outsourced labor financial plans, when applicable

Quality
- ❑ Plan is in compliance with organization regulatory requirements [R]
- ❑ Plan estimates budgetary requirements for minimum of 1 year (3-5 ideal)
- ❑ Plan is updated periodically (at least annually)
- ❑ There is a process and criteria for evaluating the quality of the financial plan [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:
FISMA Sec 3544(c)(2)(A) and (d)(1)(B) [OLRC 2003]
3544 "(c) AGENCY REPORTING—Each agency shall—
''(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—
''(A) annual agency budgets"
3544 "(d) PERFORMANCE PLAN—
(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of— […]
''(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b)."
[indirect]
FISMA Sec 3544(a)(1)(C)
3544 "(a) IN GENERAL—The head of each agency shall— […]
''(1) be responsible for—
''(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes"

Incident Management Capability Metrics
Guidance References: [indirect] NIST SP 800-65 *Integrating IT Security into the Capital Planning and Investment Control Process* [Hash 2004] Sec 1.1 Background [p 1] "FISMA, the Clinger-Cohen Act, and other associated guidance and regulations, including Office of Management and Budget (OMB) Circulars A-11 and A-130, charge agencies with integrating IT security and the capital planning and investment control (CPIC) process."
Internal Organization References:

4.2.2 Are there documented roles and responsibilities for key incident management activities throughout the organization?

This function focuses on internal organizational incident handling coordination and reporting. Incident management is the end-to-end management of any events or incidents throughout an enterprise. Participants in the protection, detection, analysis, and response processes can come from many different components of the organization. Understanding who has what roles and responsibilities for various tasks in incident management facilitates timely coordination, communication, decision-making, and problem resolution. Roles and responsibilities can be documented via an organization chart, a point-of-contact list, or some other written document. Note that this metric has a strong tie to the Interface question (0.1.1). If the interfaces are poorly defined, this function will also be difficult to meet since the actual roles and responsibilities across the organization may not be adequately defined or clarified.

Not applicable – This function may not be applicable if the organization is so small that it has only a few staff members and they interchangeably share the roles and responsibilities for incident management.

Impact statement – Knowing who is responsible for key tasks in incident management reduces confusion, streamlines communication and coordination, and ensures a comprehensive response. All of this reduces the response time, potentially limiting the damage to key assets and data from any attacks or potential threats.

Scoring and interpretation guidance – The goal of satisfactorily answering this question is to ensure that the appropriate staff members are included in incident analysis and response planning, coordination, and implementation.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] answer to this question can be achieved if
  - there is an outdated organization chart OR
  - the organization chart is in the process of being built or obtained OR
  - there is a list of POCs for key elements throughout the organization OR
  - there is a general understanding of roles and responsibilities of key incident management elements throughout the organization AND
  - these elements are consistently and appropriately contacted
- The [No] answer to this question is achieved if the majority or all of the required indicators [R] are not met.

Improvement – Improvements can be achieved by developing an up-to-date organization chart, written charter, or workflow that identifies all parties involved in incident management and their assigned roles and responsibilities. This information should be periodically reviewed and updated to include any changes in personnel and responsibilities. Improvements can also be made by making this document easily accessible in hardcopy and electronic form and including it in training materials, orientation packets, or handbooks for those involved in incident management activities, including applicable constituent members.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>4.2.2</td><td colspan="4">Are there documented roles and responsibilities for key incident management activities throughout the organization?</td><td colspan="2">Priority II</td></tr>
<tr><td rowspan="2">Not observed ❑</td><td rowspan="2">Not applicable ❑</td><td>Yes</td><td colspan="2">▪ There is a current organization chart and assigned roles and responsibilities.</td><td rowspan="2">Y ❑
P ❑
N ❑</td></tr>
<tr><td>Partial</td><td colspan="2">▪ There is an organization chart, but it is outdated and inaccurate or lacks any detailed designation of roles and responsibilities.</td></tr>
<tr><td colspan="7">Prerequisites
❑ Parent organization has an organization chart [R]
Controls
❑ Incident management personnel collect organizational and reporting structure for organization
Activity
❑ The organization chart is adapted, as needed, to meet incident management activity needs, indicating internal reporting structures and other pertinent attributes
❑ The work and information flow for incident management activities are documented (e.g., work process flows, flowcharts, procedures, etc.) including roles and responsibilities, nature of information exchanged, and any requirements associated with the interfaces between different groups [R]
Supporting Mechanisms
❑ Mechanisms to document and disseminate roles and responsibilities
Artifacts
❑ Organization organizational chart documentation [R]
Quality
❑ Organization chart is up to date [R]
❑ Organization chart or another document includes descriptions of roles and responsibilities for each key position [R]
❑ Personnel are familiar with their own roles and responsibilities as well as with the internal reporting structure for other personnel they work with [R]
❑ The allocated roles and responsibilities are periodically reviewed (at least annually) for effectiveness and efficiency and improvements are made as needed [R]</td></tr>
<tr><td colspan="7">Regulatory References: None</td></tr>
<tr><td colspan="7">Guidance References:
NIST SP 800-61 Computer Security Incident Handling Guide [Grance 2004]
Sec 2.4.4 and 3.2.7
Sec 2.4.4 Dependencies Within Organizations
[p2-13] “It is important to identify other groups within the organization that may be needed to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including— […] Management […] Information Security […] Telecommunications […] IT Support […] Legal Department […] Public Affairs and Media Relations […] Human Resources […] Business Continuity Planning […] Physical Security and Facilities Management […]”
Sec 3.2.7 Incident Notification
[p 3-16] “When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations. Timely reporting and notification enable all those who need to be involved to play their roles. […] Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates).”</td></tr>
<tr><td colspan="7">Internal Organization References:</td></tr>
</table>

4.2.3 Is there a program management plan (workforce plan) for incident management personnel?

This function focuses principally on planning staffing needs. Many incident management teams possess a core group of individuals who provide the basic level of incident handling services. Each staff member is expected to have some minimum set of basic skills to do the work and be effective in his or her work responsibilities. For example, while it is expected that any team member is able to recognize an intruder tool found in an incident, only a subset of that staff may have the skills to analyze intruder-developed exploit tools, identify and document the impact of resulting attacks, and provide insight to the rest of the team members. Thus, it is also important for the team to include or have access to experts with in-depth understanding of the technologies that the team and the constituency use. These experts, who might be in another part of the organization, can provide technical guidance or advice; they might also provide training and mentoring to other team members. This additional level of expertise is a resource that can help to broaden and deepen the technical knowledge and capabilities of the team.

If an organization is unable to find internal experts or to hire or train staff to provide the necessary specialist skills, its members may be able to develop relationships with experts in the field to provide the necessary skills. These types of creative relationships, of course, require advance negotiation and/or trusted relationships between the incident management staff and the expert(s). These relationships can be defined in formal or informal agreements (with clearly defined requirements or expectations) that outline how the request for assistance is made, and what restrictions are placed on information that is shared. When a situation arises where in-house knowledge is not sufficient, these technical specialists can be called upon to fill the gap in expertise.

When more complex incidents are reported, teams will need to supplement or expand their basic skills to include more in-depth knowledge so that staff members can understand, analyze, and identify effective responses to reported incidents.

Not applicable – This function may not be applicable if the organization is so small that it has only a few staff members and no future growth is expected, or if sufficiently well-established relations with other parts of the organization exist.

Impact statement – An organization must have the capability to meet its provided incident management service level. If that expertise is not within the organization, some mechanism must be in place to supplement or augment that capability, such as a third-party provider. If this function is successfully performed, the organization will have the right people in place to react quickly and expertly to any event or incident that threatens the organization infrastructure.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that there are staffing resources to execute the incident management mission.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] answer to this question can be achieved if
  - there is an outdated program management plan OR
  - there is program management plan currently being developed

- The [No] answer to this question is achieved if the majority or all of the required indicators [R] are not met.

Improvement – Improvements can be achieved by developing a written program plan that identifies current and future staffing requirements. This chart should be periodically reviewed and updated. An accurate plan can best be achieved by measuring current workloads, response times, and skill levels of personnel. Based on this information operational statistics can provide concrete support of staffing needs. Improvements can also be made by including as much detail as possible in the plan including number and type of personnel required, contractor support criteria, staffing skills and certifications required, and any security clearances needed.

Incident Management Capability Metrics						
4.2.3	**Is there a program management plan (workforce plan) for incident management personnel?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ There is an up-to-date program management plan documenting types and number of personnel required.	Y ❑	P ❑	N ❑
		Partial	▪ There is an out-of-date program management plan documenting the types and number of personnel required.			

Prerequisites
- ❑ An organization standard for personnel planning exists [R]

Controls
- ❑ There are defined knowledge and skill sets for employees [R]

Activity
- ❑ Quantitative operational statistics are analyzed and extrapolated to anticipate future staffing needs
- ❑ Constituency is polled for its projected needs pertaining to incident management services
- ❑ Workforce plan is documented for next 1 (minimum) through 5 (ideal) years [R]
  - Plan details the number and types of personnel required [R]
  - Plan accounts for required security clearances [R]
  - Plan includes contractor support criteria, required skills, certifications, etc.

Supporting Mechanisms
- ❑ Personnel or contractor performance data collection and analysis tools or procedures
- ❑ Workforce planning and management tools

Artifacts
- ❑ Workforce plan documentation [R]
- ❑ Collected performance data [R]
- ❑ Clearance documentation
- ❑ Contractor resumes, biographies, certifications, and other supporting documentation
- ❑ Policies and procedures for assessing performance data
- ❑ Historic record of past decisions made from performance data

Quality
- ❑ Workforce plan is updated at least annually [R]
- ❑ Workforce plan is based on extrapolated operational statistics and projected constituency needs [R]
- ❑ Workforce plan is reviewed and approved by organization management
- ❑ There is a process and criteria for evaluating the quality of the workplan [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:
FISMA Sec 3544(d)(1)(B) [OLRC 2003]
3544 "(d) PERFORMANCE PLAN—
(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of— […]
''(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b)."
[indirect]
FISMA 3544(a)(1)(C)
3544 "(a) IN GENERAL—The head of each agency shall— […]
''(1) be responsible for –"
''(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes"

Incident Management Capability Metrics
Guidance References: [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.4.3 Incident Response Personnel
Internal Organization References:

4.2.4 Is there a Quality Assurance (QA) Program to ensure quality of work and delivery for provided products and services?

This function focuses on process improvement and optimization. Having a quality assurance program in place allows the organization to gauge the success of its overall incident management capability. Ensuring that all tasks are completed effectively, that resulting products and outputs are clear, timely, and accurate, and that staff have the right skill sets and training to perform their job functions will result in an efficient organizational response capability. There may be some performance metrics and SLAs associated with key or critical services and products. These should be part of an overall quality program. Reviews of products and services can be continual (an inherent part of the work process), periodic, random, or a combination of these. A key aspect is the identification of necessary corrections and implementation of those corrections.

Note that every function in this document contains a set of quality indicators that should be incorporated into any quality assurance program as part of evaluating the quality of incident management in the organization.

Not applicable – Quality improvement is a key to the success of any function. If incident management personnel do not perform quality assurance testing, it should be done by another part of the organization or by an independent third party. This function will always be applicable.

Impact statement – Using quality reviews and incorporating feedback will improve the overall operational capability resulting in better management, faster and more effective response to threats and attacks, and ultimately, customer satisfaction.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is that the organization constantly strives to improve its incident management service quality via feedback mechanisms. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- All other combinations of indicators yields a [No] answer.

Improvement – Improvements can be achieved by building in a process to perform quality assurance reviews or tests on a periodic and consistent basis and by using the results to improve the operation of the incident management functions. Implementing a quality assurance program successfully means that personnel know and understand management's commitment to quality and understand their role in ensuring quality. Training and mentoring in a quality culture, sharing of lessons learned from quality reviews, and rewarding high-quality behavior are all actions that can improve the overall organization incident management culture and, in turn, the overall organization incident management services.

Incident Management Capability Metrics				
4.2.4	**Is there a Quality Assurance (QA) Program to ensure quality of work and delivery for provided products and services?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is a Quality Assurance Program to ensure quality of work and delivery for provided products and services.	Yes ❑	No ❑

Prerequisites

- ❑ Organization culture of measured, managed, and constant improvement and optimization exists [R]

Controls

- ❑ QA policy exists [R]
- ❑ Acceptable service levels and quality targets are established [R]
- ❑ There are defined policies and procedures for reviewing products and services for quality, reporting the results, and implementing improvements [R]
- ❑ Responsibility for quality assurance is assigned [R]
- ❑ Defined measures for performance, timeliness, accuracy, relevance/priority, and other quality criteria are defined and documented for each activity, product, and service and for each outsourced activity [R]
- ❑ Personnel are appropriately trained about the policies, procedures, and tools used to achieve and review quality in incident management products and services [R]

Activity

- ❑ Incident management activities, products and services are periodically reviewed for adherence to applicable quality measures [R]
- ❑ Quality statistics are gathered, analyzed, and reported on a periodic basis for incident management products and services [R]
- ❑ QA results are used as input into improving the quality and delivery of services [R]
- ❑ Quality criteria are periodically reviewed and adjusted [R]

Supporting Mechanisms

- ❑ QA statistics, reports, and improvement tracking tools and mechanisms [R]

Artifacts

- ❑ QA program reports or other results [R]

Quality

- ❑ QA reports are generated and reviewed periodically [R]
- ❑ QA history shows steady improvement that is in line with management expectations
- ❑ Personnel are periodically briefed on the importance of QA
- ❑ Quality is pervasive throughout the incident management groups

Regulatory References: None

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.4.2 Using Collected Incident Data [p 3-24, 3-25] "**Objective Assessment of Each Incident**. The response to an incident that has been resolved can be analyzed to determine how effective it was." "**Subject Assessment of Each Incident**. Incident response team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked—to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory. "Besides using these metrics to measure the team's success, organizations may also find it useful to periodically audit their incident response programs. Audits will identify problems and deficiencies that can then be corrected. At a minimum, an incident response audit should evaluate the following items against applicable regulations, policies, and best practices: - Incident response policies and procedures - Tools and resources - Team model and structure - Incident handler training and education - Incident documentation and reports - The measures of success discussed earlier in this section."
Internal Organization References:

4.2.5 Is there an established business resumption plan to support disaster recovery, reconstitution, and restoration efforts for incident management functions?

This function focuses on the continuity of service for incident management activities. Just like other organizational units, the incident management capability must be able to continue operations during any type of outage or disruption, even when under attack. Security and IT best practices recommend a written business resumption plan. Such a plan for incident management should include a backup site where operations can move if the primary physical location is unusable. It should also include backup and mirrored services such as DNS, mail, web services, and other communications support that are needed for daily or crisis operations. Note that the terms business resumption, continuity of operation (COOP), disaster recovery, and emergency response plans are often used interchangeably. One of these plans may exist and cover all aspects or several plans may exist to address multiple types of situations. The evaluation team needs to ask these questions carefully to determine the scope of the plans that exist and how the plans are used in supporting incident management functions.

Not applicable – Incidents can still occur under extreme and crisis situations, so incident management functions will necessarily also need to continue to operate. Even when there is not a specific plan for these functions, they should be part of overall organization disaster recovery and business resumption plans. This function will always be applicable.

Impact statement – Key service and operations must keep going in the face of a disaster. Implementing a quality business resumption plan for incident management will provide the means to be resilient during outages, attacks, or natural disasters. This ensures the security posture of the organization is consistent and not compromised during such a crisis.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is that the organization has continuous incident management support during significant crises. This is a Priority I function and the question can only have a Yes or No answer.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- All other combinations of indicators yields a [No] answer.

Improvement – Improvements can be achieved by having a documented process that is regularly reviewed, updated, and tested. The plans should be easily accessible and incident management personnel should be trained in how to initiate and follow the plans. The plans should provide for personnel safety first in the event of a disaster. The resumption plans should also be integrated with any organization disaster recovery and business resumption plans. The plan(s) should also be evaluated when organizational changes occur, such as reorganizations, mergers, and acquisitions.

Incident Management Capability Metrics				
4.2.5	**Is there an established business resumption plan to support disaster recovery, reconstitution, and restoration efforts for incident management functions?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is a documented business resumption and disaster recovery plan for systems and resources supporting incident management. This plan includes the designation of a continuity of operations (COOP) site.	Y ❑	N ❑

Prerequisites

- ❑ Organization requires incident management operational continuity of services [R]
- ❑ Mission critical incident management services, systems, personnel, and equipment have been identified and documented

Controls

- ❑ Acceptable service levels for recovery, reconstitution, and restoration activities have been identified and agreed to by organization management

Activity

- ❑ A disaster recovery plan and COOP site have been established [R]
- ❑ Established disaster recovery and business resumption plans are followed during a crisis or disaster [R]
- ❑ Scenario-based exercises are periodically conducted to test plans (contingency, business resumption, disaster recovery, emergency response, etc.) [R]

Supporting Mechanisms

- ❑ Means for moving primary operations to COOP site, as required (e.g., personnel, computing infrastructure, email, phone, etc.) to alternate site

Artifacts

- ❑ A plan that addresses continuity of operations such as [R]
  - business resumption plan
  - contingency plan
  - disaster recovery plan
  - emergency response plan

Quality

- ❑ Plans contain provisions to continue operations at another site if necessary [R]
- ❑ Plans are tested, improvements are made, and results are documented [R]
- ❑ Plans are updated periodically and reviewed at least annually
- ❑ Employees are familiar with the plans [R]
- ❑ Plans provide for safety of personnel first in the event of a disaster
- ❑ There is a process and criteria for evaluating the quality of this plan [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(8) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—

''(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

Guidance References: None

[indirect]

NIST SP 800-34 *Contingency Planning Guide for Information Technology Systems* [Swanson 2002]

Internal Organization References:

4.2.6 Is there a personnel security plan for incident management personnel?

This function indicates whether there is an overarching personnel security plan that covers such topics as background checks, qualification verification, and security clearances for those involved in incident management activities.

Not applicable – Constituencies require trust in the incident management personnel. They need to ensure that staff have integrity and will not put the team or organization at risk. If the incident management group or team does not perform this function, this metric should be applied to the part of the organization that does. This function should always be applicable.

Impact statement – Implementing a program plan that sets a level of personnel qualifications, security, and organization-required personnel clearances ensures that there are qualified, trusted personnel to do the work. This provides an environment in which staff members can successfully perform their operations, increasing the security posture of the organization.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to provide appropriately cleared/checked staffing.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.
- The [Partial] answer to this question can be achieved if
  - there is a program management personnel security plan that may be outdated OR
  - the organization is in the process of building such a program management or planning is underway
- The [No] answer to this question is achieved if the majority or all of the required indicators [R] are not met.

Improvement – Improvements can be achieved by developing a written program plan that identifies required personnel security qualifications and clearances. This plan should be periodically reviewed and updated. This plan could be integrated into the hiring policies and practices and could also be applied to contractors.

Incident Management Capability Metrics						
4.2.6	**Is there a personnel security plan for incident management personnel?**			**Priority III**		
Not observed ❑	Not applicable ❑	Yes	▪ There are documented personnel security policies and procedures for personnel performing incident management functions.	Y ❑	P ❑	N ❑
		Partial	▪ There are practiced, but informal and undocumented personnel security policies and procedures for personnel performing incident management functions.			

Prerequisites

- ❑ Organization requires personnel security program [R]

Controls

- ❑ There are requirements for each relevant level of personnel security regarding access to physical space, data, and computing systems and the performance of specific activities related to incident management [R]
- ❑ There is a comprehensive set of program management processes and procedures for topics including [R]
  - personnel qualifications
  - personnel security
  - organization-required personnel clearances

Activity

- ❑ Pre-employment screening conducted and results filed in human resources (HR)
- ❑ Personnel have been indoctrinated to personnel security responsibilities
  - initial security briefing
  - annual refresher briefing

Supporting Mechanisms

- ❑ Repository for policies and procedures for employees to search, read, and review policy documentation
- ❑ Security clearance custodial services for storing and passing clearances in compliance with organization standards [R]

Artifacts

- ❑ Documented policies and procedures on file, including [R]
  - employee screening policies and procedures
  - clearance requirement documentation
- ❑ Personnel clearance records for employees as well as contractors (if appropriate)

Quality

- ❑ Policy is reviewed at least annually and updated as needed
- ❑ Policy is accessible to all employees
- ❑ All or most personnel and contractors requiring clearances have been completed and are up to date (e.g., background investigations finished, no interim clearances)
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

[indirect]

FISMA Sec 3544(a)(4) [OLRC 2003]

3544 "(a) IN GENERAL—The head of each agency shall— […]

''(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems* [Swanson 1998] Sec 5.MA.1 Personnel Security [p 27]
Internal Organization References:

4.2.7 Is the incident management IT infrastructure adequate to support incident management functions?

This function focuses on the IT infrastructure used to support incident management activities. This is usually a separate infrastructure where there is a specifically designated CSIRT; however, some ad hoc or smaller teams may use the organization's general infrastructure for their work and may only have a small collection of special tools or equipment. The incident management infrastructure includes

- physical location and security of incident management staff and data
- staff office and home equipment
- incident management networks, systems, and internal/external defenses such as routers, firewalls, and IDS
- incident management tools and applications to support incident handling and other provided services
  - databases, data repositories, and data analysis tools for storing incident management information
  - mechanisms or applications for secure email and voice communications

Incident management facilities and network and telecommunications infrastructure must be designed with great care to protect the sensitive data that is collected. Staff will need equipment for the various functions they perform. This might include the following:

- access to secure telephones, faxes, and any intranet, extranet, or virtual private network (VPN)
- work equipment such as telephones, office computing systems, laptops, projectors, notification systems, cellular telephones, pagers, shredding machines, and electronic whiteboards
- tools for the activities being performed including incident, artifact, vulnerability analysis and handling, and other analysis tasks (such as fusion, retrospective, or correlation)
- incident tracking systems and vulnerability databases

Not applicable – All organizations require the right infrastructure to perform incident management functions. This function will always be applicable; however, it is possible that the infrastructure used for incident management activities is largely or completely the same as the general constituent infrastructure.

Impact statement – Without appropriate tools, technologies, and security defenses, incident management personnel cannot meet the expectations of the organization or constituency they serve.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that incident management personnel have the IT infrastructure necessary to support the tasks that they are chartered to perform.

- The [Yes] answer to this question can be achieved only if all of the required indicators [R] are met.

- The [Partial] answer to this question can be achieved if
  - the organization is in the process of upgrading its incident management infrastructure AND
  - funding has been allocated

Improvement – Improvements can be achieved by developing an infrastructure and corresponding funding plan to ensure that incident management personnel have the tools they need, that people and data are adequately protected, and that the ability to plan for future growth and updates is realized. Other improvements can be achieved by

- implementing a certification and accreditation program for all systems and networks used by incident management personnel
- following all best security practices regarding patch management and configuration management
- putting in place the appropriate internal and external defenses such as firewalls, IDS, routers, network monitoring for the incident management infrastructure
- looking for economies of scale in purchasing
- keeping any licenses for software and hardware up to date

Incident Management Capability Metrics						
4.2.7	**Is the incident management IT infrastructure adequate to support incident management functions?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ The incident management IT infrastructure effectively supports incident management operations.	Y ❑	P ❑	N ❑
		Partial	▪ The incident management IT infrastructure is in the process of being upgraded. Funding has been allocated and upgrades ordered.			

Prerequisites

- ❑ None

Controls

- ❑ There is a process for determining, documenting, submitting, and authorizing improvements to incident management IT infrastructure (either a separate process or part of normal organization processes) [R]

Activity

- ❑ Incident management personnel or management determine their own IT infrastructure requirements [R]
- ❑ Improvements and upgrades are identified, planned, requested, acquired, and implemented [R]
- ❑ Funding is allocated for incident management IT infrastructure elements [R]
- ❑ Funding is allocated for improving and sustaining operations (such as equipment, technical materials, security publications, professional training)

Supporting Mechanisms

- ❑ Equipment acquisition process [R]
- ❑ Certification and accreditation plan R]
- ❑ Technical reference library with check out/in record keeping
- ❑ Hardware/software lifecycle and configuration management mechanism defined [R]

Artifacts

- ❑ Long-term strategic development plan or upgrade plan for infrastructure [R]
- ❑ Inventory of IT infrastructure components [R]
- ❑ Hardware/software license documentation [R]
- ❑ Hardware/software lifecycle and configuration management plan [R]
- ❑ Recent operations testing results documentation
- ❑ Certification and accreditation plan documentation with historic records [R]
- ❑ Up-to-date technical reference library
- ❑ Training CDs and documentation
- ❑ Records of all training materials

Quality

- ❑ Hardware and software inventory is up to date and accurate [R]
- ❑ All licensing is up to date and accurate [R]
- ❑ Configuration management is independently reviewed and assessed periodically (at least annually) [R]
- ❑ Personnel are familiar with and adhere to the lifecycle and configuration management plan
- ❑ All equipment certifications and accreditations are up-to-date [R]
- ❑ The adequacy of the incident management IT infrastructure is periodically reviewed and improvements are requested [R]

Regulatory References: None

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems* [Ross 2004] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.1.1 Preparing to Handle Incidents [p 3-2] Table 3-1 Tools and Resources for Incident Handlers
Internal Organization References:

4.3 CND Technology Development, Evaluation, and Implementation

4.3.1 Is there a capability to safely test software tools for use within the incident management environment?

This function focuses on validating and verifying the safety of the tools, technology, software, and hardware used to support incident management activities (including sensors, data analysis tools, event/incident handling/tracking tools, malicious code detection tools, IDS, IPS, firewalls, routers, system upgrades, etc.) and making sure they do not introduce vulnerabilities into the environment. Any tools that are going to be deployed for use must be tested to ensure that they perform as expected and do not interact in unexpected ways with existing software, hardware, and applications.

Not applicable – TBD

Impact statement – The most serious impact for not safely testing tools is that the organization's systems can be compromised. If a tool is implemented without checking its behavior, this can lead to loss of revenue, loss of customer trust, and loss of protected or proprietary information. Vulnerable systems could be attacked and used as launch platforms for other abuses, which could lead to legal liabilities for the organization.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that any tools (software or hardware, new operating system versions, etc.) are tested prior to being installed and/or implemented in production network(s).

- The [Yes] answer for this question can be achieved if all required indicators [R] are met.
- The [Partial] grade for this question can be achieved if
  - there are procedures that mandate how new tools are introduced into the incident management environment AND
  - there are informal procedures for completing this task AND
  - personnel follow the informal procedures in a consistent manner AND
  - there are mechanisms in place (configuration management, change management, etc.) to enable poorly implemented changes to be "backed out" OR
  - the organization is developing a test-bed/laboratory for such testing
- Any other combination of indicators is a [No].

Improvement – Other indicators not listed above are additional measures of high-quality operations and do not affect the grade for this metric. They are ideas for improving the effectiveness and quality of the activities described in this metric. Improvements for this function can also be achieved by implementing

- plans for the development of a capability for testing new software/hardware, tools, equipment, etc.
- a formalized process for evaluating new software, technologies, etc.
- a plan for developing formal procedures, guidelines, and best practices for testing software for use in the incident management environment

Incident Management Capability Metrics						
4.3 CND Technology Development, Evaluation, and Implementation						
4.3.1	**Is there a capability to safely test tools for use within the incident management environment?**			**Priority III**		
Not observed ❑	Not applicable ❑	Yes	▪ There is a test-bed capability to safely evaluate tools. ▪ Performance and usefulness of tools to support incident management activities is reviewed	Y ❑	P ❑	N ❑
		Partial	▪ A test-bed capability for safe evaluation of incident management tools is being planned or designed. ▪ Other trusted sources are depended on to provide evaluation of new tools.			

Prerequisites

- ❑ Isolated (non-production) network exists to test tools, new software/hardware and other technology prior to deploying for production use [R]
- ❑ Tools are obtained from trusted partners/sources and limited additional testing is performed

Controls

- ❑ Guidelines exist that explain how the tools should be evaluated and tested to support incident management activities [R]
- ❑ Documented policies and procedures exist for obtaining, testing, and deploying tools within the incident management environment [R]
- ❑ Procedures mandate that new software, technologies, etc., must be evaluated and tested prior to deployment within the incident management infrastructure [R]
- ❑ Process exists to review the performance and usefulness of software tools (e.g., sensor data analysis, incident/event handling, malicious code detection)

Activity

- ❑ Trusted or tested suite of tools are used to perform incident management activities [R]
- ❑ Documented test results of products assessed in the test-bed environment exist

Supporting Mechanisms

- ❑ Configuration management system for software and tools [R]
- ❑ Change management system for software and tools [R]
- ❑ Patch management system for software and tools [R]

Artifacts

- ❑ List of tools that have been tested and are allowed to be used in production networks [R]

Quality

- ❑ Staff have a technical understanding and knowledge of the software, tools, databases, etc. supporting incident management activities [R]
- ❑ Staff are aware of, knowledgeable of, and consistently follow the procedures for this activity [R]
- ❑ There are documented performance reports on file for tools that have been tested
- ❑ There is a process and criteria (including those defining adequate testing is for incident management tools) for evaluating the quality of this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Incident Management Capability Metrics
4.3 CND Technology Development, Evaluation, and Implementation
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 3.1.1 Preparing to Handle Incidents [p 3-2] Table 3-1 Tools and Resources for Incident Handlers Incident Analysis Hardware and Software: "**Spare workstations, servers, and networking equipment**, which may be used for many purposes, such as restoring backups and trying out malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software."
Internal Organization References:

4.3.2 Is there a process to monitor and review various forms of media to ensure that incident management personnel stay abreast of emerging technologies?

This function focuses on the need for incident management personnel to stay current with the environment in which they and their constituency work. It is important to be aware of new types of technology that may be embraced by the team or members of its constituency. They should seek such information from a variety of sources, including reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can also include communicating with other parties that are authorities in these fields to ensure that the most accurate information or interpretation is obtained. As such emerging technologies are incorporated into the organization's infrastructure, incident management personnel will need to become knowledgeable about how the technology works. They need to know about any special considerations for their implementation or integration with other systems or networks and any information that may indicate potential threats and problems.

Not applicable – It is possible that this function might be outsourced or handled by another part of the organization. If so, then this metric should be applied to that group and its activities. If this function is not performed anywhere within the organization, then this function can be marked as Not Applicable.

Impact statement – The danger in not keeping abreast of new or emerging technologies that may be incorporated into the organization's systems is that when (not if) incidents, attacks, or threats occur, the incident management activities may fail to appropriately handle the situations; this can result in a risk to the organization's assets and its ability to continue to do business.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that incident management personnel regularly monitor a variety of security, news, and other trusted sites for information relating to new and emerging computing technologies.

- The [Yes] answer to this question is achieved when all of the required indicators [R] are met.
- The [Partial] grade for this question can be achieved if
  - the organization is in the process of developing such a capability or service OR
  - incident management personnel infrequently monitors such news sources for emerging technology OR
  - there are informal procedures for completing this task AND
  - personnel understand and follow the informal procedures consistently

Improvement – Improvements can be achieved by building a strategy for learning about new technologies. This can include having staff members participate in

- vendor presentations, conferences, or demonstrations
- organizational discussions on new equipment purchasing plans (to understand what skills and knowledge will be needed to support changes in the operating environment)
- professional development activities for staff to learn new skills (e.g., classes, conferences)

Incident Management Capability Metrics						
4.3.2	**Is there a process to monitor and review various forms of media to ensure that incident management personnel stay abreast of emerging technologies?**			**Priority IV**		
Not observed ❑	Not applicable ❑	Yes	▪ There is a documented process to monitor and review various forms of media to stay abreast of emerging technologies.	Y ❑	P ❑	N ❑
		Partial	▪ There is an undocumented, ad hoc process to monitor and review various forms of media.			

Prerequisites

- ❑ None

Controls

- ❑ Policies and procedures detail how information is to be reviewed, collected, synthesized, disseminated, and used [R]
- ❑ A documented checklist exists that catalogs which sites to visit and the types of information to examine
- ❑ Documented safeguards and instructions exist for reviewing content on high-risk web sites such as "black-hat" sites [R]

Activity

- ❑ Personnel check a variety of web sites or email lists on a daily or weekly basis for information on emerging technologies [R]
- ❑ Personnel extract and synthesize information gathered [R]
- ❑ Personnel communicate with organization personnel and management to discuss emerging technologies [R]

Supporting Mechanisms

- ❑ Email systems and mailing lists
- ❑ Technology periodicals or other resource media
- ❑ RSS news feeds with targeted information

Artifacts

- ❑ Product evaluation reports on file
- ❑ Records of information gathered [R]
- ❑ Archives of emails from mailing list subscriptions
- ❑ Research and analysis reports based on the information gathered
- ❑ Periodic vendor product demos or technologies on site

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Personnel are aware and knowledgeable about methods for identifying appropriate information sources for emerging technologies [R]
- ❑ There is a process and criteria for evaluating the quality of performance and results (e.g., information on emerging technologies is up to date and accurate) associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References: None

[indirect]
NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 2.5 Incident Response Team Services

Internal Organization References:

4.4 Personnel

4.4.1 Are there established ETA requirements and minimum competency levels incorporated into the training program for all personnel performing incident management activities?

This question focuses on the need to have established criteria to provide training for incident management personnel (for new staff as well as continued training for existing staff). To be successful, it is critical that personnel have the requisite knowledge, skills, and abilities to perform their tasks in support of their mission and goals, as well as the constituency being served. This includes training for specific tasks, tools, and procedures relative to incident management functions.

Not applicable – It is unlikely that an organization would indicate a "not applicable" response to this question, unless the training program was handled by another part of the organization. Even so, the organization must identify its needs for the technical knowledge, skills, and abilities that are required to perform incident management tasks.

Impact statement – With proper requirements for ETA and minimum competency levels incorporated into the training program, an organization can be assured it will have the right staff with the appropriate skills, abilities, and knowledge to effectively handle the depth and breadth of incident management tasks. Without these ETA requirements, the security posture of the entire organization could be at risk for failure.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that incident management personnel have received the training they need, that they have the education and awareness needed, and that they have the range of skills required. It is also necessary that the staff members understand their working environment and are able to use the tools that support their assigned roles and responsibilities in the performance of incident management activities.

This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory grading of this metric [Yes] can be achieved if all the required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvements can be made by developing matrices for all roles and responsibilities involved in incident management and determining the range of technical and/or management knowledge, skills, and abilities needed to effectively perform these activities, and by developing training plans that will expose the staff to the requisite ETA requirements. Other improvements can involve determining requirements for appropriate levels for certifications or other professional degrees including proficiency in a specific technology or capability. "Incentivizing" staff to continue to develop professional knowledge, skills, and abilities through bonuses or promotions can be another driver for improvements.

Incident Management Capability Metrics				
4.4 Personnel				
4.4.1	**Are there established ETA requirements and minimum competency levels incorporated into the training program for all personnel performing incident management activities?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There are established ETA requirements, standards, and minimum competence levels incorporated in the training program, in compliance with regulations and requirements.	Yes ❑	No ❑

Prerequisites

- ❑ A training program exists that identifies technical training requirements and competency levels for personnel, both government and contractor as appropriate [R]

Controls

- ❑ Training procedures state that training is mandatory [R]
- ❑ Guidelines exist that explain the ETA requirements (type, frequency, etc.) [R]
- ❑ Documented policies and procedures describe the training requirements, schedules, etc.

Activity

- ❑ Personnel coordinate training schedules with their management [R]
- ❑ Personnel periodically (at least annually) identify new training or skills that are needed [R]
- ❑ Personnel or management identify when additional training is needed
- ❑ Security policies and other IT-related issues (e.g., physical, personnel, operations security) are covered in new employee introduction/training [R]

Supporting Mechanisms

- ❑ Mechanism to validate that training is completed, tracked, and recorded for each employee's training requirements, and that qualifications and deficiencies are noted (e.g., test results, certificates, records of CBT access, database, spreadsheet, etc.) [R]
- ❑ Online training products available through CDs and/or Intranet, distance learning opportunities, local/classroom environments, etc.

Artifacts

- ❑ List(s) of recommendations and information resources on training topics, courses, conferences, etc., that personnel can select from
- ❑ Training records on file [R]
- ❑ Goals for technical training are spelled out in the training program for incident management personnel
- ❑ Personnel can demonstrate their knowledge, skills, and abilities to perform the technical work (show how they use the tools, how logs are analyzed, access databases, explain what training they have received, etc.)

Quality

- ❑ **All** incident management employees have received initial IT security and awareness training, training on roles/responsibilities for incident management functions, etc. [R]
- ❑ Annual refreshers for security awareness and other relevant training requirements are provided [R]
- ❑ Personnel are knowledgeable and aware of their training needs and work with management to obtain any needed training/education/awareness
- ❑ Funding is allocated for external technical training and professional development for all of its personnel (this might include contracted employees, when such training is not covered in the contract)
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
4.4 Personnel
Regulatory References: None [indirect] FISMA Sec 3544(a)(3)(D) and (a)(4) [OLRC 2003] 3544 "(a) IN GENERAL—The head of each agency shall— […] ‘‘(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— […] ‘‘(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; […] ‘‘(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.4.3 Incident Response Personnel [p 2-12 and 2-13] "Members of the incident response team should have excellent technical skills […] Every team member should have good problem solving skills […]It is important to counteract staff burnout by providing opportunities for learning and growth. […] Incident response team members should have other skills in addition to technical expertise. Teamwork skills […] good communication skills. Speaking skills […] Writing skills [...]"
Internal Organization References:

4.4.2 Is there a professional development program for incident management personnel?

This function focuses on the continued, professional development of incident management staff. Note that there may be different programs in place for organization personnel and contractor personnel. In order for this function to be effectively performed, all personnel performing incident management functions should have professional development options.

Not applicable – TBD

Impact statement – A sense of lacking a career path can increase the amount of personnel turnover.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to support further professional development of staff. Establishing an approach for developing a career or growth path will help to ensure that personnel remain committed to the work and have a way to increase their knowledge and skills. In addition, exposing personnel to other information assurance or computer network defense training will increase their awareness of security-related issues. Personnel should be able to participate in professional development activities as part of the overall protection, detection, response, and sustainment of activities.

- The [Yes] answer to this question can be achieved if all the required indicators [R] are met.
- A [Partial] answer to this question can be achieved if the organization
  - provides limited opportunities for personnel to participate in internal or external professional development programs AND
    - has guidance (preferably documented policies and procedures) that define how personnel participate in professional development activities AND
    - participates in information assurance or other CND-related forums (technical exchanges, FIRST, conferences, etc.) OR
  - shares information/resources with colleagues and incident management staff to raise awareness within the team AND
    - has a reference collection of training and documentation for use by incident management personnel AND
    - participates in government/industry information assurance or other CND-related forums (technical exchanges, FIRST, conferences, etc.) AND
    - has a mechanism for scheduling participation in such events AND
    - reviews professional development activities with personnel on an annual (or other periodic timeframe) basis
- Any other combination of indicators is insufficient and results in a [No].

Improvement – The overall effectiveness of incident management activities can be improved if there is a defined plan or program that includes professional development of staff skills and knowledge that enables individuals to progress along their career paths.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>4.4.2</td><td colspan="4">Is there a professional development program for incident management personnel?</td><td colspan="2">Priority IV</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ There is both an internal and external professional development program for incident management personnel.</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ There are only limited opportunities for incident management personnel to participate in internal OR external professional development programs.</td></tr>
<tr><td colspan="7">Prerequisites
❑ None
Controls
❑ Participation in professional development activities is a documented goal for the organization and, as applicable, contractor personnel [R]
❑ Guidelines that explain professional development program exist
❑ Documented policies and procedures exist that delineate how personnel participate in professional development activities [R]
❑ Documented check-out, usage, and return procedures for training materials
Activity
❑ Personnel share information/resources with colleagues and incident management staff to raise awareness within the team [R]
❑ Personnel participate in IA or other CND related forums [R]
❑ Funding is allocated for purchase of latest, relevant technical books and materials for staff
Supporting Mechanisms
❑ Mechanisms for requesting and authorizing participation in such events [R]
❑ Database for tracking professional activities for personnel/team accomplishments [R]
❑ Organization-owned and centrally managed IA/CND training and documentation reference library for training material
Artifacts
❑ Schedule for appropriate technology or IA forums for planned participation
❑ Material received at forums (presentations, documents, handouts, CD’s, other media)
❑ Personnel records for professional development schedules [R]
❑ Examples of forms to request professional development
❑ Collection of various IA/CND awareness information
❑ Reference library check-out/usage/return procedures
Quality
❑ Annual (or other interim) review of professional development activities [R]
❑ There is a process and criteria for evaluating the quality of performance and artifacts (e.g., the effectiveness of training materials, classes, forums etc.) associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
</table>

Incident Management Capability Metrics
Regulatory References: None [indirect] FISMA Sec 3544(a)(3)(D) and (a)(4) [OLRC 2003] 3544 "(a) IN GENERAL—The head of each agency shall— […] ''(3) delegate to the agency Chief Information Officer established under Section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— […] ''(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; […]" ''(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.4.3 Incident Response Personnel [p 2-12] "It is important to counteract staff burnout by providing opportunities for learning and growth."
Internal Organization References:

4.5 Security Administration

4.5.1 Are there physical protective measures in place to protect incident management IT systems, facilities, and personnel?

This function focuses on the measures implemented to protect incident management IT systems, facilities (e.g., rooms or buildings), and personnel who perform incident management functions. Since incident management personnel will be collecting, accessing, and storing sensitive information that relates to its constituency, it is important that there are appropriate physical controls over the environment to protect these systems. In many cases, this becomes the "example of best practice behaviors" for the rest of the constituency, and as a result is held to a higher standard. These practices usually address protection not only of the IT systems, but also the physical space and the personnel working in that space. Access cards, for example, protect an entire area, including people and equipment.

Not applicable – It is unlikely that there would be a "not applicable" statement for this function, since the organization must show evidence that it is protecting its incident management systems and facilities and the critical information contained therein, as well as its personnel.

Impact statement – A compromise or unauthorized access to any incident management information will have a profound, negative effect on the reputation of the incident management capability. Such loss of credibility can result in the total failure of the group or team to continue, or to be perceived by the constituency as not providing a valued service. Protecting the IT systems, infrastructure, and personnel is essential to the success of the incident management capability.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to protect the incident management systems and information held therein. The measure of success will be realized by understanding the level and extent to which strategies are implemented to protect incident management information assets (IT systems, incident management systems, operating environment, incident management personnel, etc.). This is a Priority I function and the question can only have a Yes or No answer.

- A passing score [Yes] can be achieved if all the required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No] score.

Improvement – Improvements can be achieved by defining controls for restricting access to critical resources with need-to-know requirements. Some of the non-required supporting mechanisms can be implemented to make the protective measures more robust (e.g., camera/monitoring service for visual access, swipe cards with anti-pass back features, etc.).

Incident Management Capability Metrics				
4.5 Security Administration				
4.5.1	**Are there physical protective measures in place to protect incident management IT systems, facilities, and personnel?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There are physical protective measures in place, including lockable rooms or building, access controls, and alarms.	Y ❑	N ❑

Prerequisites

- ❑ Physical protective measures for incident management IT systems and physical space have been identified [R]
- ❑ An up-to-date, accurate, and complete list of all incident management critical information and networks exists [R]

Controls

- ❑ There are documented, up-to-date policies and procedures for physical security that describe the process and method by which the incident management IT systems and physical environment are protected [R]
- ❑ Personnel are appropriately trained on the procedures for physical security [R]
- ❑ Personnel are trained on how to identify insecurities [R]
- ❑ Personnel understand the procedures for reporting insecurities [R]
- ❑ There are documented policies and procedures for admitting visitors to facilities
- ❑ Appropriate asset tagging or labeling is used to support inventory management

Activity

- ❑ Procedures for protection strategies exist [R]
- ❑ Personnel understand their day-to-day security responsibilities [R]
- ❑ Personnel follow physical protection strategies [R]

Supporting Mechanisms

- ❑ Access controls for visitors (escort requirements, badges, etc.) [R]
- ❑ Biometric devices
- ❑ Alarms (e.g., fire, flood, entry, or other alarmed devices) [R]
- ❑ Restricted hours [R]
- ❑ TV Cameras
- ❑ Swipe cards, 24 x 7 guard
- ❑ Safes, sensitive systems in secured areas [R]

Artifacts

- ❑ Current lists of authorized individuals who have access to area(s) [R]
- ❑ Up-to-date list of management POCs to notify under specific conditions [R]
- ❑ Examples of any forms for changes in protection measures

Quality

- ❑ Personnel are aware of and understand protection measures and the need for them [R]
- ❑ Personnel receive annual "refresher" training on protection measures [R]
- ❑ There is a process and criteria for evaluating the quality and effectiveness of protection measures [R]
- ❑ The quality and effectiveness of this activity are periodically (monthly, semi-annually, annually, or when conditions warrant) evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(3) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—

''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 6.2.2 Incident Prevention [p 6-2] Table 6-1 Actions to Prevent Unauthorized Access Incidents "Physical Security: Implement physical security measures that restrict access to critical resources."
Internal Organization References:

4.5.2 Is there an operations security (OPSEC) program?

This function focuses on identifying and protecting information that might provide attackers with information about the incident management plans or capabilities.

Not applicable – This function may be marked as Not Applicable if this operations security activity is handled by some other part of the organization and if the evaluator is able to confirm that OPSEC training has occurred for staff and the staff can demonstrate knowledge and awareness of OPSEC.

Impact statement – Personnel are sufficiently aware of operations security to protect their information assets.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is to ensure that incident management personnel are sensitive to how information and data are created, handled, stored, retained, archived, and destroyed, and that they recognize the importance of operations security in protecting that data and information. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory score [Yes] can be achieved if all the required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No] score.

Improvement – Some improvements that can be made include

- scheduling speakers to present case studies or other scenarios
- using other methods (e.g., contests) to educate personnel about OPSEC
- conducting periodic walkthroughs of the physical workspaces to review and identify potential insecurities

Incident Management Capability Metrics				
4.5.2	**Is there an operations security (OPSEC) program?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is a documented operations security (OPSEC) program.	Yes ❑	No ❑

Prerequisites
- ❑ Operations Security Program has been established [R]
- ❑ Identified critical information and indicators are identified [R]

Controls
- ❑ Documented policies and procedures exist that provide guidance on protecting potentially exploitable information [R]
- ❑ Information about the operations security program including roles, responsibilities, and POCs exists and is available to all personnel [R]
- ❑ Methods exist for identifying critical information, analyzing potential threats, identifying risks and determining countermeasures [R]
- ❑ Defined processes exist for visitor access to areas where critical incident management activities occur

Activity
- ❑ Personnel receive formal/informal OPSEC training, briefings, and information [R]
- ❑ Personnel receive refresher training (monthly, quarterly, semi-annually, etc.) [R]
- ❑ Personnel integrate OPSEC as part of their day-to-day culture [R]
- ❑ Operations security flyers or other awareness aids are posted or distributed

Supporting Mechanisms
- ❑ Mechanisms for reporting OPSEC failures (templates, forms, processes, procedures [R]
- ❑ Mechanisms for providing information to the personnel (web, email, posters, meetings, presentations, etc.) [R]

Artifacts
- ❑ Samples of OPSEC awareness materials, guidance, templates for reporting failures/other insecurities, etc. [R]
- ❑ Videos, flyers, posters, and other awareness aids such as mouse pads, magnets, or buttons

Quality
- ❑ OPSEC information is up to date, accurate, and relevant [R]
- ❑ Personnel have an understanding and knowledge of OPSEC [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None
[indirect]
FISMA Sec 3544(b)(3) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.6 Recommendations [p 2-16] "Establish policies and procedures regarding incident-related information sharing."
Internal Organization References:

4.6 CND Information Systems

4.6.1 Are there Defense-in-Depth strategies and methodologies to harden the incident management computer networks and systems?

This function focuses on the ability of the incident management capability to identify multiple layers of security protection strategies in the hardening of its own systems, network, and information assets.

Not applicable – It is unlikely that an organization would not have some type of plan in place to protect the incident management assets. This function should never be "Not Applicable."

Impact statement – There should be a strategy that ensures that there are no single points of failure in the protection of the systems and networks that support incident management activities. The resulting in-depth defenses limit the opportunities for attacks, threats, and vulnerabilities to be successful in breaching security.

Scoring and interpretation guidance – The question is fully satisfied when the organization has a defined Defense-in-Depth strategy that has been implemented to protect its incident management assets. This is a Priority I function and the question can only have a Yes or No answer.

- A [Yes] answer for this metric is achieved if all the required indicators [R] have been met.
- Any combination of other indicators is a [No].

Improvement – Improvements can be achieved by

- conducting quality assurance tests or checks of security products and tools to ensure they are current and up to date
- conducting mock exercises to test defense-in-depth methods and determine if they are working
- implementing products from different vendors to provide more robust coverage to avoid single points of failure, for example, from the anti-virus products; using products from competing vendors on PCs and servers or multiple anti-virus products on the same devices.
- if any in-house tool development is done, implementing code reviews and testing for insecurities (security "walkthroughs")

Incident Management Capability Metrics				
4.6 CND Information Systems				
4.6.1	**Are there Defense-in-Depth strategies and methodologies to harden the incident management computer networks and systems?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Defense-in-Depth methodologies and strategies are utilized in hardening of its own computer systems and networks.	Y ❑	N ❑

Prerequisites

- ❑ Defense-in-Depth strategies and methodologies for incident management systems and networks have been defined [R]

Controls

- ❑ There is a documented, known strategy for implementing and maintaining appropriate defense-in-depth [R]
- ❑ Documented, up-to-date, policy for Defense-in-Depth strategy exists [R]
- ❑ Documented, up-to-date procedures for implementing Defense in Depth exist [R]
- ❑ Documented policies and procedures defining method and mechanisms for installing, replacing, updating/upgrading systems and networks to improve Defense in Depth exist [R]
- ❑ There are identified POCs and assigned roles and responsibilities for defensive actions [R]
- ❑ Personnel are appropriately trained on the procedures and relevant Defense-in-Depth methods and technologies [R]
- ❑ Personnel understand how to report insecurities or failures in any defense mechanisms [R]

Activity

- ❑ Designated personnel review, maintain, and update components, documents, and procedures for Defense in Depth [R]
- ❑ Defense-in-depth strategy is periodically tested for effectiveness and completeness and improvements are made as needed [R]

Supporting Mechanisms

- ❑ Multiple tiers of security exist for incident management networks and working environments, for example [R]
  - Physical security is in place [R]
  - Host and network based IDS and/or IPS are in place on incident management mission critical systems are installed [R]
  - Firewalls are in place for perimeter security [R]
  - DMZ is set up for public web, DNS, and email servers [R]
  - Anti-virus software is installed on all workstations and critical servers [R]
  - Content security monitoring tools are installed [R]
  - Access control lists are used [R]

Artifacts

- ❑ Rule sets for IDS/IPS [R]
- ❑ Schedules for or automatic updates enabled for monitoring tools [R]
- ❑ Schedule for AV signature updates [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures
- ❑ Defense-in-Depth ETA is implemented for all incident management personnel, with annual refreshers
- ❑ There is a process and criteria (including the effectiveness, completeness, and scope of the defense-in-depth strategy, methods, and technologies) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
4.6 CND Information Systems
Regulatory References: None [indirect] FISMA Sec 3544(b)(3) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"
Guidance References: None [indirect] NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Swanson 1996] NIST SP 800-18 *Guide to Developing Security Plans for Information Technology Systems* [Swanson 1998]
Internal Organization References:

4.6.2 Are there processes and technologies to support the confidentiality, integrity, and availability of incident management data and information?

This function focuses on the ability of the organization to protect the confidentiality, integrity, and availability (C/I/A) of its data and information, not only for incident management but also for any constituent information that incident management personnel receive, handle, transmit, store, or archive.

Not applicable – It is unlikely that this function would be Not Applicable, since an organization should have a plan in place to protect its assets.

Impact statement – Without effective measures to protect information and ensure it hasn't been modified, deleted, or inappropriately accessed, there is potential risk to the organization. Sensitive information collected as part of incident management activities (e.g., vulnerable systems or personal information) needs to be protected to ensure it has not been "tainted," viewed, copied, modified, or deleted. Having robust protection strategies in place to protect these assets will maintain confidential information, ensure it is available to those who are authorized to see and use it, and ensure it has not been inappropriately modified.

Scoring and interpretation guidance – Satisfactory performance of this function is evident when the organization has well-defined policies and procedures in place for protective and defensive strategies, and when the personnel are knowledgeable about, consistently use, and support the repeatable processes for handling information commensurate with the various security levels. This is a Priority I function and the question can only have a Yes or No answer.

- A [Yes] answer for this metric is achieved if all the required indicators [R] have been met.
- Any combination of other indicators is a failure [No].

Improvement – Improvements can be achieved by

- incorporating encryption solutions for off-site storage of backup and archive data
- arranging risk assessments, conducting self-assessments, or using independent evaluations to validate processes and procedures for how data and information are handled, processed, transmitted, accessed, stored, and destroyed
- reviewing all of the non-required indicators to identify those that can be part of an improvement strategy for "raising the bar" for processes and technologies to provide a more robust support for confidentiality, integrity, and availability for data and information

Incident Management Capability Metrics				
4.6.2	**Are there processes and technologies to support the confidentiality, integrity, and availability of incident management data and information?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There are processes and technologies to support confidentiality, integrity, and availability of data and information.	Y ❑	N ❑

Prerequisites

- ❑ There are defined requirements for the confidentiality, integrity, and availability of data and information [R]

Controls

- ❑ Documented, up-to-date policy, procedures, and processes exist for protecting the confidentiality, integrity and availability of data and information [R]
- ❑ Personnel are appropriately trained on the procedures and relevant technology [R]
- ❑ All personnel are trained on how to respond to any events or anomalous activities

Activity

- ❑ Appropriate technology [e.g., public key infrastructure (PKI), PGP, GnuPG, or secure virtual private networking (VPN), secure mail/voice/FAX] is used to secure the transmission of sensitive information between the constituent and incident management functions, and any external entities (sites, regulatory bodies, law enforcement, etc.) [R]
- ❑ Data are appropriately protected at all times during collection, transmission, storage, review, and manipulation [R]
- ❑ There is access to secure data storage to support C/I/A of data and information, such as [R]
  - secure fire-proof, water-proof containers for storage of backup tapes
  - remote storage of backups for disaster recovery
  - all backups stored outside of the computer room in a secure, access controlled room with fire and environmental safeguards
  - backups labeled appropriately

Supporting Mechanisms

- ❑ Appropriate technology to support CIA during transmission, processing, storage (e.g., AV software on workstations and servers) [R]
- ❑ Backups (files, equipment, application software)

Artifacts

- ❑ Results from monitoring audit files (to ensure protective/detection tools are functioning as expected)
- ❑ Physical and electronic protection measures (safes, ACLs, shredders, evidence of use of encryption, etc.) [R]

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity [R]
- ❑ There is a process and criteria (including timeliness and accuracy) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:

FISMA Sec 3544(b)(3) [OLRC 2003]

3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—

''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Swanson 1998] NIST SP 800-18 *Guide to Developing Security Plans for Information Technology Systems* [Swanson 1998]
Internal Organization References:

4.6.3 Do incident management personnel monitor their own systems and networks?

This function focuses on the ability of incident management personnel to ensure they are watching their own networks.

Not applicable – It is possible that the monitoring of these systems and networks is done by another part of the organization. The evaluator should confirm that the required [R] indicators outlined in this question are performed by that other group.

Impact statement – Monitoring can provide early warnings about malicious threats or activity in their infrastructure, allowing a timely response and containing the potential damage. This improves the network defense posture of the team's internal systems and ultimately the organization it serves and allows it to provide an agile response.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is an effective plan implemented for monitoring incident management systems to protect information assets. This includes methods for detecting events/incidents, anomalous activity, intrusion attempts, and other potential threats. This is a Priority I function and the question can only have a Yes or No answer.

- A [Yes] answer for this metric is achieved if all the required indicators [R] have been met.
- Any combination of other indicators is a failure [No].

Improvement – The optional or non-required indicators relative to network security monitoring identify areas where improvement in quality, timeliness, and accuracy can occur. This might include

- using automated tools
- ensuring automated alerts are enabled
- implementing multiple types of network monitoring systems
- ensuring results are analyzed in near real time
- ensuring network diagrams of monitoring system placement are available and up to date

Incident Management Capability Metrics				
4.6.3	**Do incident management personnel monitor their own systems and networks?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Monitoring is conducted on incident management systems and networks.	Y ❑	N ❑

Prerequisites

- ❑ There is an up-to-date, accurate, and complete list of all critical incident management systems, data, and information [R]

Controls

- ❑ Documented policies and procedures for monitoring networks exist and include [R]
  - detailed instructions for characterizing anomalous events, including suspicious ports, protocols, and services (both network based and host based) [R]
  - roles/responsibilities and timeframes for reviewing IDS logs after an event for preliminary analysis [R]
  - a requirement to review audit logs upon receipt
- ❑ Personnel are trained in the procedures and technical tools used for monitoring the systems and networks [R]
- ❑ Reports of analyses are available and disseminated to appropriate individuals [R]
- ❑ Network diagrams showing IDS placement on incident management network(s) exist
- ❑ Only authorized users have access to systems and networks [R]

Activity

- ❑ Network monitoring tools are installed and used [R]
- ❑ Network and host-based IDS are installed and used [R]
- ❑ Logs are reviewed after detection of an event or potential incident [R]
- ❑ Log files are reviewed as required for other analyses
- ❑ The common operating picture is periodically reviewed and updated
- ❑ Reports or alerts/notifications are forwarded to other organizations as appropriate [R]
- ❑ Personnel are assigned to perform batch and/or real-time analysis on data collected from its networks [R]
- ❑ 24 x 7 analysis/support cell exists
- ❑ Personnel are assigned to perform maintenance, software upgrades, configuration updates [R]

Supporting Mechanisms

- ❑ Behavior-based IDS performs heuristic scanning for unauthorized activity [R]
- ❑ Anti-virus software performs heuristic scanning for malicious code detection [R]
- ❑ Monitoring tools have automated alert capability [R]
- ❑ ADS system, or an ADS plug-in to an IDS system [R]
- ❑ Intrusion detection system signature databases are up to date [R]
- ❑ Mechanism for controlling access (e.g., foreign nationals, visitors) to systems [R]

Artifacts

- ❑ Logs, alerts, and reports generated by the network monitoring tools [R]
- ❑ Network diagrams showing placement of monitoring tools on constituent networks
- ❑ Recent monitoring audit logs [R]
- ❑ Reports from monitoring activities [R]
- ❑ Results of testing of monitoring on critical network segments
- ❑ IDS configuration file specifying what anomalous events trigger an alarm

Incident Management Capability Metrics
Quality Indicators: ❑ Backup and recovery capabilities in the form of spare equipment for IDS sensors/console exist [R] ❑ Monitoring data is analyzed on a regular basis (real-time, hourly, etc.) [R] ❑ Alert capabilities include appropriate communication mechanisms, including page-out and email alerts [R] ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R] ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
Regulatory References: None [indirect] FISMA Sec 3544(b)(3) [OLRC 2003] 3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"
Guidance References: None
Internal Organization References:

4.6.4 Are Risk Assessments (RAs) performed on incident management systems and networks?

This function focuses on the ability of the organization to perform risk assessments on incident management systems, networks, and practices. This includes having a capability for

- public and private monitoring of information sources and organizations (such as CERT/CC, vendor sites, and other similar organizations) for information about risk assessments
- keeping up to date on current vulnerability threats, attacks, and remediation strategies (through research, training, mentoring, and attending courses and other forms of professional development)
- coordinating with other internal and external parties to schedule, conduct, and review results of such assessments
- properly reporting to approved individuals and/or upper management
- implementing fixes and mitigation for risks identified during analysis (this includes categorizing, prioritizing, and assessing the impact to incident management systems)

Organizational collaboration and coordination will require internally defined processes, roles, and responsibilities.

Not applicable – This function should never be Not Applicable. The incident management capability should stand as an exemplar for the rest of the organization on proactive detection and correction of weaknesses.

Impact statement – A thorough risk assessment provides a valuable means of proactively identifying and mitigating risks in technology, process, and people, before such weaknesses can be exploited.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is that the organization is able to consistently, accurately, and reliably conduct risk assessments on its incident management internal systems and networks, and to implement strategies to remove or mitigate any risks. This is a Priority I function and the question can only have a Yes or No answer.

- The satisfactory grading of this metric [Yes] can be achieved if all required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No].

Note that the prerequisite states that incident management personnel have approval (from management or other authorized individuals) to conduct such assessments; however, if they do not perform this activity, it is possible that some other part of the organization does it on behalf of them. Regardless of whoever performs the assessments, current documentation and information on the systems criticality and the assets on those systems must be identified. Without this information, risk or threat can only be evaluated in an abstract, theoretical sense.

Improvement – One possible improvement is to perform certification and accreditation of incident management systems and networks as a means of reducing risk.

Incident Management Capability Metrics				
4.6.4	**Are Risk Assessments (RAs) performed on incident management systems and networks?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Risk assessments are periodically performed on incident management systems and networks.	Y ❑	N ❑

Prerequisites
- ❑ Management (or other authorized body) has given approval for risk assessments to be conducted on the CSIRT systems and networks [R]
- ❑ List of critical incident management systems, data, and information [R]

Controls
- ❑ Documented policies and procedures exist that describe the process and method by which risk assessments are conducted and the results are analyzed [R]
- ❑ Personnel are appropriately trained on the procedures, process and supporting technologies used to conduct risk assessments and corresponding analysis [R]

Activity
- ❑ Risk assessments are conducted on incident management systems/networks [R]
- ❑ A list of risk assessment methodologies (e.g., NIST guidance, COBIT, OCTAVE®) is collected, maintained, and updated
- ❑ RA results are provided to the appropriate individuals [R]
- ❑ RA results are documented, analyzed, tracked, and recorded [R]
- ❑ RAs are used to determine potential impacts and to make improvements to CND infrastructure to prevent computer security incidents [R]

Supporting Mechanisms
- ❑ Available, approved risk assessment tools/methods used in accordance with organization requirements [R]
- ❑ Mechanism for tracking and reporting risks and corrective actions [R]

Artifacts
- ❑ Copies of records, analysis or results of risk assessments [R]
- ❑ List of risk assessment types and providers with POC lists

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ Designated schedule is followed for performing risk assessments (on a periodic/scheduled basis, when new systems are acquired, when there is an organizational change that impacts incident management activities/systems, etc.)
- ❑ RA results are archived in a secure and protected manner [R]
- ❑ Any communications of the RA results are done in a secure and protected manner [R]
- ❑ There is a process and criteria (including completeness, frequency, adequacy, scope, and level of detail for RAs) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:
FISMA Sec 3544(b)(1) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
''(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency"

Incident Management Capability Metrics
Guidance References: None [indirect] NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems* [Swanson 2001]
Internal Organization References:

4.6.5 Are vulnerability scanning tools run on incident management systems and networks?

This function focuses on whether the organization performs vulnerability scanning on incident management systems and networks to identify potential threats and problems. This scanning may be done by a CSIRT or by another group of individuals within the organization that is responsible for performing such activities. In either case, management authorization must be obtained (preferably in written form), describing the conditions and schedule under which such activities are performed.

Policies and procedures should identify the guidelines and rules for scheduling, conducting, analyzing, and taking action on any information identified as a result of such scanning activity.

Not applicable – It is possible that this function might be outsourced or handled by another part of the organization (see above). If this is the case, then this question should then be applied to that group and its activities.

Impact statement – Such scanning can provide warnings about weaknesses that may have an impact on the incident management infrastructure. Results from this vulnerability scanning can be used as rationale for updates or changes in system/network configurations, or as justification for new components, system upgrades, or additional software/hardware.

Scoring and interpretation guidance – This function is fully satisfied when the organization conducts vulnerability scanning of incident management systems on a routine schedule (a periodic schedule, such as daily, weekly, monthly, and whenever a potential threat warrants). This is a Priority I function and the question can only have a Yes or No answer.

- A [Yes] answer for this metric can be achieved if all required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- formalized procedures, guidelines, and training covering how to provide notification and how to determine if the scanning will interfere with other incident management operations (situational awareness)
- quality assurance checks on the information provided by the scans to ensure that it is complete, timely, accurate, clear and understandable, up to date, useful, and meets any organization, institutional, or legal compliance guidelines
- automated tools for performing vulnerability scanning and tracking, including a vulnerability database that allows tracking of vulnerabilities by organizational or constituent unit, along with the ability to track vulnerability remediation

Incident Management Capability Metrics				
4.6.5	**Are vulnerability scanning tools run on the incident management systems and networks?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ Vulnerability scanning tools are routinely run on incident management systems networks, and when warranted.	Y ❑	N ❑

Prerequisites
- ❑ Authorizations to perform vulnerability scanning have been provided (by procedures, documented roles and responsibilities, MOUs, email, policy, etc.) [R]
- ❑ List of systems containing critical assets and data exists [R]

Controls
- ❑ Documented policies and procedures exist that describe the process and method by which vulnerability scanning is conducted [R]
- ❑ Documented policies and procedures exist that define reporting requirements
- ❑ Personnel are appropriately trained on the procedures, processes, and supporting technologies used to conduct vulnerability scanning (or others who perform such activities have those qualifications) [R]

Activity
- ❑ A list of POCs for notification and alert is maintained [R]
- ❑ Sources for robust tools and information used in vulnerability scanning are reviewed
- ❑ Remediation, response, and recovery solutions to address findings in results of vulnerability scans are implemented [R]
- ❑ Documentation on changes/update is provided
- ❑ Information on vulnerability scanning is tracked and recorded [R]

Supporting Mechanisms
- ❑ Available, approved vulnerability scanning tools (NMap, ILook, etc.) used in accordance with organization requirements [R]
- ❑ Mechanisms for tracking and monitoring vulnerability scanning activities and archiving results [R]

Artifacts
- ❑ Vulnerability scan reports [R]
- ❑ POC list of authorized individuals who perform the vulnerability scanning [R]

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ A designated schedule for performing vulnerability scanning (or more often as warranted) is followed
- ❑ There is a process and criteria (including timeliness, completeness, adequacy, and frequency of vulnerability scans) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References:
FISMA Sec 3544(b)(5) [OLRC 2003]
3544 "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]
''(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
''(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under Section 3505(c); and
''(B) may include testing relied on in a evaluation under Section 3545"

Incident Management Capability Metrics
Guidance References: NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2-14, 2-15] "**Vulnerability Assessment**. An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. These responsibilities can be extended so that the team performs auditing or penetration testing, perhaps visiting sites unannounced to perform on-the-spot assessments. Incident handlers are well suited to performing vulnerability assessments because they routinely see all kinds of incidents and have first-hand knowledge of vulnerabilities and how they are exploited. However, because the availability of incident handlers is unpredictable, organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource."
Internal Organization References:

4.6.6 Is there a patch management program in place for the incident management systems?

This function focuses on whether there is a defined process for receiving alerts about patches, installing patches, monitoring installation to ensure patches were correctly installed on incident management systems and networks, and determining how to handle any exceptions or extensions when patching cannot be implemented immediately.

Incident management personnel can actually install the patches on their own systems or another group within the organization can have that authority.

Incident management personnel should seek information about patch notifications from as many sources as needed, including CERT/CC, software and hardware vendors, other vulnerability analysis and reporting organizations, and other security experts. Tracking all such notices, the impacts on the incident management systems, and the actions taken in a database or tracking system can help to keep a history of vulnerability actions for the team and can provide a source mechanism for trend analysis.

It may not always be possible to patch a system, or to conduct sufficient testing to ensure a patch will work as expected on that system. Incident management personnel need to know which systems fall into these categories and ensure that appropriate actions are taken to prevent patches from affecting operational production systems, or ensure that appropriate mitigation actions are taken to monitor and defend unpatched systems.

Not applicable – This function should never be Not Applicable.

Impact statement – Timely patch alerts and installation provide a method to protect systems from threats. Patch management can help increase the security posture of the organization by protecting critical incident management systems, networks, and data.

Scoring and interpretation guidance – This function is fully satisfied when notice of new patches is received, the appropriate incident management personnel are notified, patches are downloaded, tested, and installed, and there are appropriate documented policies and procedures and training on conducting these activities.

This is a Priority I function and the question can only have a Yes or No answer. Specifically, the scoring guidance is as follows:

- A [Yes] answer for this metric can be achieved if all required indicators [R] are met.
- Any other combination of indicators is insufficient and results in a [No].

Improvement – Improvement can be achieved by implementing

- formalized procedures and guidelines
- quality assurance checks on the information provided to ensure that it is complete, timely, accurate, clear, understandable, up to date, useful, and meets any organization, institutional or legal compliance guidelines
- training for personnel on the patch mitigation and installation techniques and methodologies
- a process to keep all POC lists and security mailing list subscriptions up to date
- automated tools for patch dissemination and installation

Incident Management Capability Metrics				
4.6.6	**Is there a patch management program in place for the incident management systems?**			**Priority I**
Not observed ❑	Not applicable ❑	▪ There is a patch management program in place for the incident management systems.	Y ❑	N ❑

Prerequisites
- ❑ Inventory of critical incident management systems, data, and information are available [R]
- ❑ Inventory of systems that cannot be patched due to business, compliance, or other reasons is available [R]

Controls
- ❑ Documented, up-to-date policy and procedures for patch management exist (including assigned roles and responsibilities) [R]
- ❑ Documented procedures for testing patches exist [R]
- ❑ Primary and secondary responsible personnel for patch management are designated [R]
- ❑ Personnel are trained on the procedures and relevant technology [R]

Activity
- ❑ Personnel obtain/download patches from a trusted, approved, or authorized site [R]
- ❑ Personnel test patches (use a test server or test-bed where patches can be loaded and tested, verify checksum, ensure patch doesn't cause failures, etc.) [R]
- ❑ The organization is on the CERT/CC, vendor, and other security group lists for patch notifications (including the technical advisories) and actively receives patch information and alerts [R]
- ❑ Appropriate vendor, external contacts, and constituency are notified about any corrupt software packages
- ❑ Patch extension requests are documented, particularly describing rationale and identifying potential technical risks and mitigation strategies [R]
- ❑ Processes are in place to monitor, analyze, and conduct remediation on unpatched systems [R]
- ❑ Reports are generated on patch implementation

Supporting Mechanisms
- ❑ Automated tools for distributing and installing patches on incident management systems and networks
- ❑ Mechanism for reporting/recording patch compliance/notification [R]
- ❑ Guidance for patch installation [R]
- ❑ Communication mechanisms for patch notification [R]
- ❑ Cost effective means of meeting patch compliance requirements (e.g., automated tools, templates, forms, or data collection mechanisms)

Artifacts
- ❑ Copies of reports sent to intermediate organization group as appropriate [R]
- ❑ Confirmation receipts (for patches) from other entities when applicable
- ❑ Notification lists for any management or personnel to be contacted

Quality
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task [R]
- ❑ Personnel are aware and knowledgeable about patch installation, patch monitoring, and remediation strategies for unpatched systems [R]
- ❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Incident Management Capability Metrics
Regulatory References: None [indirect] FISMA 3544(b)(3) [OLRC 2003] 3544 “(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— ‘‘(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]”
Guidance References: NIST SP 800-40 *Procedures for Handling Security Patches* [Mell 2002] Sec 2 Creating and Implementing a Patching Process [p 5] “We recommend creating a "Patch and Vulnerability Group" (PVG).” and Sec 5 Patching Procedures NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004] Sec 2.5 Incident Response Team Services [p 2.15] “**Patch Management**. Giving the incident response team the responsibility for patch management (e.g., acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization) is generally not recommended. Patch management is a time-intensive, challenging task that cannot be delayed every time an incident needs to be handled. In fact, patch management services are often needed most when attempting to contain, eradicate, and recover from large-scale incidents. Effective communication channels between the patch management staff and the incident response team are likely to improve the success of a patch management program.”
Internal Organization References:

4.6.7 Is there an alternate communications system (other than email) for receiving and distributing notifications, information about incidents, and other kinds of warnings?

This function measures the ability of the organization to contact all relevant parties whenever necessary.

Not applicable – It would be unusual for this function to be Not Applicable since most common services provide at a minimum phone and email capabilities for notification. Even a minimalist "call tree" backup plan could be implemented. The evaluator should capture any rationale if this function is going be marked as Not Applicable.

Impact statement – Communications channels can fail in unexpected ways. As a proactive measure, alternative means of communication must be established and tested to ensure proper communications during emergencies or time-critical activities.

Scoring and interpretation guidance – The function is fully satisfied when there are documented policies, procedures, and guidance for implementing or maintaining alternate communications systems. The function is partially satisfied if communications depend on a primary method or share a common point of failure (e.g., email servers and alternate systems are on same network). Specifically, the scoring guidance is as follows:

- The [Yes] answer for this question can be achieved if all required indicators [R] are met.
- The [Partial] answer for this question can be achieved if
  - the organization has informal procedures, limited, or an ad hoc process for implementing alternate communications OR
  - personnel understand and follow the informal procedures consistently
- The [No] answer for this question results if most or all of the required indicators [R] are not met.

Improvement – Improvement can be achieved by implementing

- formal procedures, guidelines, and training, including how to implement alternative communications processes and methods, notification, and how to follow the methodology
- a process to keep all POC lists and source information up to date

Incident Management Capability Metrics						
4.6.7	**Is there an alternate communications system (other than email) for receiving and distributing notifications, information about incidents, and other kinds of warnings?**			**Priority II**		
Not observed ❑	Not applicable ❑	Yes	▪ There are multiple mechanisms for receiving and distributing information about new viruses, incidents, vulnerabilities, and threats.	Y ❑	P ❑	N ❑
		Partial	▪ Voice/FAX is used as the alternate communications system.			

Prerequisites

- ❑ Multiple communication methods have been identified and implemented [R]

Controls

- ❑ Documented policies requiring periodic testing of communications exist [R]
- ❑ Policies and procedures outline roles, responsibilities, scope, appropriate tools, and notification requirements [R]
- ❑ Documented guidance for each type of communication method exists [R]
- ❑ Personnel are appropriately trained on the procedures, process, and supporting technologies used [R]

Activity

- ❑ An alternate communications system and plan are maintained [R]
- ❑ Appropriate personnel are notified during operational exercises per the test communications plan
- ❑ Contingency plan provides for alternate means of communications [R]
- ❑ COOP provides measures to maintain communications through almost any emergency or disaster
- ❑ Various forms of communications are used such as pagers, mobile phones, FAX, STU III, secure email, alternate email account(s) on separate networks, secure web page exist, for emergency communications
- ❑ Any Voice over Internet Protocol (VoIP) issues in contingency plan are considered, as well as their limitations

Supporting Mechanisms

- ❑ Web, email, telephone, mobile, two-way radio, FAX, pager, etc.
- ❑ Contact lists with alternate contact info for designated personnel [R]

Artifacts

- ❑ Demonstration of alternate communications paths
- ❑ Results and lessons learned from testing communications mechanisms
- ❑ POC list with appropriate organizations, and trusted agents to contact [R]

Quality

- ❑ Defined criteria, including when to implement alternate methods, exist [R]
- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ Periodic testing and evaluation of communications availability is performed (monthly, semi-annually, or when service providers change)
- ❑ More than one alternate communications method exists

Regulatory References: None

Guidance References:

NIST SP 800-61 *Computer Security Incident Handling Guide* [Grance 2004]
Sec 3.2.7 Incident Notification [p 3-16] "The team should plan and prepare several communication methods, and select the methods that are appropriate for a particular incident."

Internal Organization References:

4.7 Threat Level Implementation

4.7.1 Is the latest organization or other relevant guidance and procedures for threat level reporting process, formats, directive actions, and security accessible, maintained, and followed?

This function focuses on the ability of the organization to implement a comprehensive process for effectively handling changes in threat levels. Threat levels can be national in origin, such as those established by the U.S. Department of Defense (sometimes referred to as INFOCON levels) or some other external entity warnings that are applicable to the organization. As part of any protection strategy, incident management personnel must be able to manage and track changes in response to threat level status for incident management systems and networks and be able to quickly implement changes in requirements associated with increasing or decreasing threat levels.

Not applicable – It would be unusual for this function to be Not Applicable since that would imply that incident management personnel never notify anyone in the organization about changes in threat levels. The evaluator should capture the rationale for this function to be classified as Not Applicable and use judgment to decide if the rationale is valid or not. If is the reason is not valid, this question should be marked as not met.

Impact statement – Adhering to threat guidance and directives can help ensure that people and technology (systems and networks) are focused on aligning their actions to adapt to changes that can affect a variety of operational issues: personal protection, protection of data and information, and the resilience of the systems for continued operations.

Scoring and interpretation guidance – The goal of satisfactorily performing this function is for the organization to have an established mechanism in place that enables it to alter its operational activities to meet increasing or decreasing security postures and for personnel to perform their roles and responsibilities to meet the mission, goals, and objectives for incident management. This is a Priority I function and the question can only have a Yes or No answer.

- A score [Yes] can be achieved if all of the required indicators [R] are met.
- Any other combination of indicators results in a [No] score.

Improvement – The optional or non-required indicators relative to threat level processes identify possible areas for improvement planning. Other possible improvements include

- formalizing POC lists and periodic validation to ensure up-to-date information is available during changes in threat levels
- performing mock exercises and using lessons learned to improve processes

Incident Management Capability Metrics				
4.7.1	**Is the latest organization or other relevant guidance and procedures for the threat level reporting process, formats, directive actions, and security accessible, maintained, and followed?**		**Priority I**	
Not observed ❑	Not applicable ❑	▪ The latest organization or other relevant guidance and procedures are maintained and adhered to for the threat level reporting process, formats, directive actions, and security.	Y ❑	N ❑

Prerequisites

- ❑ Information is received about threat levels from the organization or other appropriate sources [R]
- ❑ Defined criteria on when to implement threat level changes exist [R]

Controls

- ❑ Documented procedures exist for managing and tracking threat level status (both elevating and de-escalating levels) [R]
- ❑ Procedures are in compliance with appropriate regulations or guidance [R]
- ❑ Personnel have technical understanding of ramifications associated with threat levels (for increasing or decreasing) [R]
- ❑ Procedures provide detailed guidance on steps to change threat levels, including roles and responsibilities and notification requirements [R]

Activity

- ❑ Personnel review changes in threat level reporting guidance
- ❑ Personnel follow threat level reporting guidance
- ❑ Personnel change threat levels based on threat situation and guidance instructions [R]

Supporting Mechanisms

- ❑ Mechanism for tracking compliance exists [R]
- ❑ Assigned POCs to change threat levels [R]

Artifacts

- ❑ Copies of latest organization threat level procedures [R]
- ❑ Up-do-date list of POCs to be notified or involved in threat changes [R]
- ❑ Guidance procedures or measures to implement when changing threat levels [R]
- ❑ Demonstration of changes in threat levels (exercises, scenarios, table top walkthroughs)
- ❑ Reports with tracking and implementation of security threat level on internal networks

Quality

- ❑ Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task [R]
- ❑ There is a process and criteria (e.g., information is up to date and current) for evaluating the quality of performance and artifacts associated with this activity [R]
- ❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]

Regulatory References: None

Guidance References: None

Internal Organization References:

4.7.2 Is the constituency assisted with decisions regarding changes to local threat levels?

This function focuses on the ability of incident management personnel to help their constituency with changes in threat levels by providing assistance and guidance, and by monitoring the changes to support any reporting requirements or regulations. Threat levels can be national in origin, such as those established by the Department of Homeland Security (or some other external entity warnings that are applicable to the organization) or local. For example, there may be a specific threat level associated with an incident that only affects the city or area in which part of the organization resides. As part of any protection strategy, incident management personnel must be able to quickly help its constituency implement changes in requirements associated with such changes in local threat levels—whether that level is increasing or decreasing.

Not applicable – It is unlikely that this function would be Not Applicable since even at the organizational level there should be a plan or process in place to determine appropriate changes in operations based on threat levels within the constituency.

Impact statement – TBD

Scoring and interpretation guidance – The metric is fully satisfied when there are documented policies, procedures, and guidance for assisting constituents with changes in threat levels.

- The [Yes] answer for this question can be achieved if all required indicators [R] are met.
- The [Partial] grade for this question can be achieved if
  - there are informal procedures for completing this task OR
  - incident management personnel assist the constituents with guidance and technical support for threat level changes on an occasional basis AND
  - personnel understand and follow the informal procedures consistently AND
  - feedback on lessons learned is sent to the appropriate contacts

Improvement – Improvement can be gained by instituting

- quality assurance testing
- policies to document and test all procedures
- training in procedures and threat levels

Improvements in efficiency can also occur by maintaining and updating a prioritized list of criteria for how threat level changes affect the constituents' networks and by using this list to determine primary contacts. Further improvements can be achieved by assessing the impacts of threat changes on the constituency's mission and operations.

<table>
<tr><th colspan="7">Incident Management Capability Metrics</th></tr>
<tr><td>4.7.2</td><td colspan="4">Is the constituency assisted with decisions regarding changes to local threat levels?</td><td colspan="2">Priority II</td></tr>
<tr><td rowspan="2">Not observed
❑</td><td rowspan="2">Not applicable
❑</td><td>Yes</td><td>▪ Assistance is provided to constituency concerning recommendations on increasing local threat levels as conditions warrant (including providing information on threats, warnings, and incidents).</td><td rowspan="2">Y
❑</td><td rowspan="2">P
❑</td><td rowspan="2">N
❑</td></tr>
<tr><td>Partial</td><td>▪ The constituency is provided with assistance on an ad hoc basis.</td></tr>
<tr><td colspan="7">Prerequisites
❑ Information is received about threat levels from the organization or appropriate sources [R]
❑ Incident management personnel are aware of and understand the threat levels and their meanings [R]
Controls
❑ Documented procedures exist for managing and tracking threat level status (both elevating and de-escalating threat levels) for constituent systems [R]
❑ Documented protective measures required for each threat level exist [R]
❑ Documented policies and procedures for assisting constituents in applying threat changes exist [R]
❑ Personnel are appropriately trained on the policies and procedures for providing assistance to constituents [R]
❑ Guidance includes impact assessment of threat change on constituent mission and operations
❑ Procedures are in compliance with appropriate regulations or guidance [R]
❑ Personnel have technical understanding of ramifications associated with increasing or decreasing threat levels [R]
❑ Procedures provide detailed guidance on steps to change threat levels, including roles, responsibilities, and notification requirements [R]
Activity
❑ Technical guidance is developed or provided to constituents on implementing directed measures to protect their networks in response to changing threat levels [R]
❑ Awareness and training are provided to constituency on how to respond to threat level changes
❑ Guidance includes impact assessment of threat change to constituent mission and operations
❑ Constituent compliance with threat level changes is monitored [R]
❑ Appropriate contacts are notified (through proper channels) of status, as required [R]
Supporting Mechanisms
❑ Mechanism for tracking compliance
❑ Assigned POCs (primary and backups) at constituent sites for notification [R]
Artifacts
❑ Copies of latest organization threat level procedures [R]
❑ Up-do-date list of POCs (primary and backups) to be notified or involved in threat changes [R]
❑ Guidance procedures or measures to implement when threat levels change [R]
❑ Copies of supplemental threat procedures developed by constituents
❑ Copies of lessons learned and/or follow-up reports showing that improvements were incorporated.
❑ Copies of supplemental constituent procedures on file
Quality
❑ Personnel are aware of, knowledgeable of, and consistently follow the procedure, processes, and technologies for performing this task [R]
❑ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
❑ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]</td></tr>
</table>

Incident Management Capability Metrics
Regulatory References: None
Guidance References: None
Internal Organization References:

Appendix List of Incident Management Functions

This appendix contains a simple list of all of the function questions contained in this document. It is provided for convenience for those who wish to have a complete list.

Question	Priority
Interfaces	
0.1.1 Have well-defined, formal interfaces for conducting agency incident management activities been established and maintained?	I
Protect	
Risk Assessment Support	
1.1.1 Are Risk Assessments (RAs) performed on constituent systems?	I
1.1.2 Are the constituents assisted with correcting problems identified by Risk Assessment (RA) activities?	III
1.1.3 Is proactive vulnerability scanning (VS) performed on constituent networks and systems?	I
1.1.4 Is the constituent assisted with correcting problems identified by vulnerability scanning (VS) activities?	III
1.1.5 Is trend analysis supported and conducted?	III
Malware Protection Support	
1.2.1 Is there an institutionalized Malware/Anti-Virus (AV) Program?	I
Computer Network Defense Operational Exercises	
1.3.1 Are operational exercises conducted to assess the security posture of the organization?	III
1.3.2 Are lessons learned from operational exercises incorporated into the constituents' network defenses?	III
Constituent Protection Support and Training	
1.4.1 Is there a list of which systems, data, and information are mission critical?	I
1.4.2 Is guidance provided to constituents in best practices for protecting their systems and network?	III
1.4.3 Are constituents provided with security education, training, and awareness (ETA)?	II

Question	Priority
Information Assurance/Vulnerability Management	
1.5.1 Is there a patch alert and management program?	I
Detect	
Network Security Monitoring	
2.1.1 Is there network monitoring of the security of constituent systems and networks?	I
Indicators, Warning, and Situational Awareness	
2.2.1 Are network and system configurations or rule sets reviewed and updated in response to changes in the threat environment, and are the constituents notified of the updates?	I
2.2.2 Is public monitoring of external web sites and other trusted sources of information conducted?	I
Respond	
Incident Reporting	
3.1.1 Are incidents reported to and coordinated with appropriate external organizations or groups in accordance with organizational guidelines?	I
3.1.2 Are incidents reported to appropriate organization management in accordance with organizational guidelines?	I
3.1.3 Are events/incidents reported from the constituency?	I
3.1.4 Is a notification service provided to constituents?	I
3.1.5 Are incidents reported to law enforcement as required and/or the intelligence community as appropriate?	I
3.1.6 Is there support for incident management for classified or sensitive information, networks, and/or systems?	I
3.1.7 Is there a central repository for constituent security event/incident reporting?	II
Incident Response	
3.2.1 Is there an event/incident handling capability?	I
3.2.2 Is there an operations log or record of daily operational activity?	II
3.2.3 Is information on all events/incidents collected and retained in support of future analytical efforts and situational awareness?	II
3.2.4 Is relevant information on all events/incidents collected and retained in support of law enforcement investigations?	I

Question	Priority
3.2.5 Are general incident response guidelines, checklists, and recommended procedures distributed to constituents to encourage consistency in response methods/standards?	II
3.2.6 Are trusted relationships maintained with internal organizational experts who can give technical and non-technical advice and information?	IV
3.2.7 Have trusted relationships been developed with other external experts (CERT/CC, FIRST, vendors, other entities, etc.)?	III
Incident Analysis	
3.3.1 Is incident analysis conducted?	I
3.3.2 Is fusion analysis (analyzing data from disparate sources) to identify concerted attacks and shared vulnerabilities performed?	III
3.3.3 Is retrospective analysis conducted?	IV
3.3.4 Is incident correlation performed?	II
3.3.5 Is forensics analysis performed on constituent systems and networks?	IV
3.3.6 Do the analytical processes incorporate methods to determine the risk or threat level of a confirmed incident?	I
Sustain	
MOUs and Contracts	
4.1.1 Is there an incident management function or CSIRT designated by the organization head or CIO through an official appointment order?	II
4.1.2 Is there a documented agreement(s) that identifies the incident management services provided to the constituency?	II
4.1.3 Does the agreement with the constituent specify that the constituency will provide notification in advance of changes or planned outages to its network?	III
Project/Program Management	
4.2.1 Is there a financial plan for incident management functions?	IV
4.2.2 Are there documented roles and responsibilities for key incident management activities throughout the organization?	II
4.2.3 Is there a program management plan (workforce plan) for incident management personnel?	II
4.2.4 Is there a Quality Assurance (QA) Program to ensure quality of work and delivery for provided products and services?	I

Question	Priority
4.2.5 Is there an established business resumption plan to support disaster recovery, reconstitution, and restoration efforts for incident management functions?	I
4.2.6 Is there a personnel security plan for incident management personnel?	III
4.2.7 Is the incident management IT infrastructure adequate to support incident management functions?	II
CND Technology Development, Evaluation, and Implementation	
4.3.1 Is there a capability to safely test tools for use within the incident management environment?	III
4.3.2 Is there a process to monitor and review various forms of media to ensure that incident management personnel stay abreast of emerging technologies?	IV
Personnel	
4.4.1 Are there established ETA requirements and minimum competency levels incorporated into the training program for all personnel performing incident management activities?	I
4.4.2 Is there a professional development program for incident management personnel?	IV
Security Administration	
4.5.1 Are there physical protective measures in place to protect incident management IT systems, facilities, and personnel?	I
4.5.2 Is there an operations security (OPSEC) program?	I
CND Information Systems	
4.6.1 Are there Defense-in-Depth strategies and methodologies to harden the incident management computer networks and systems?	I
4.6.2 Are there processes and technologies to support the confidentiality, integrity, and availability of incident management data and information?	I
4.6.3 Do incident management personnel monitor their own systems and networks?	I
4.6.4 Are Risk Assessments (RAs) performed on incident management systems and networks?	I
4.6.5 Are vulnerability scanning tools run on the incident management systems and networks?	I
4.6.6 Is there a patch management program in place for the incident management systems?	I
4.6.7 Is there an alternate communications system (other than email) for receiving and distributing notifications, information about incidents, and other kinds of warnings?	II

Question	Priority
Threat Level Implementation	
4.7.1 Is the latest organization or other relevant guidance and procedures for the threat level reporting process, formats, directive actions, and security accessible, maintained, and followed?	I
4.7.2 Is the constituency assisted with decisions regarding changes to local threat levels?	II

Acronyms

ACL	access control list
ADS	anomaly detection system
AV	anti-virus
CBK	Common Body of Knowledge
CBT	computer based training
CD	compact disc
CERT/CC	CERT Coordination Center
CIA	confidentiality, integrity, and availability
CIO	chief information officer
CISSP	Certified Information Systems Security Professional
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CND	computer network defense
CNDSP	computer network defense service provider
COBIT	Control Objectives for Information and related Technology
CSIRT	computer security incident response team
DHS	Department of Homeland Security
DMZ	demilitarized zone
DNS	Domain Name System
DoD	Department of Defense
ETA	education, training, and awareness
FAX	facsimile
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FTP	file transfer protocol
GnuPG	GNU Privacy Guard
HR	human resources
IA	information assurance
IC	intelligence community
IDS	intrusion detection system
IEC	International Electrotechnical Commission
INFOCON	information operations condition
IP	Internet Protocol
IPS	intrusion prevention system, or intrusion protection system
$(ISC)^2$	International Information Systems Security Certification Consortium
ISO	information security officer
ISO	International Organization for Standardization
ISP	internet service provider
IT	information technology
ITGI	Information Technology Governance Institute
ITIL	IT Infrastructure Library
LE	law enforcement
LOA	letter of agreement
MO	modus operandi (mode of operation)
MOA	memorandum of agreement
MOU	memorandum of understanding

MSSP	managed security service provider
NIC	network information center
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NOC	network operations center
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OMB	Office of Management and Budget
OPSEC	operations security
OS	operating system
PC	personal computer
PGP	Pretty Good Privacy
PKI	public key infrastructure
POC	point of contact
QA	quality assurance
RA	risk assessment
SEI	Software Engineering Institute
SKiP	Security Knowledge in Practice
SLA	service level agreement
SME	subject matter expert
SOC	security operations center
STU	secure telephone unit
TBD	to be determined
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
VPN	virtual private network
VS	vulnerability scanning

Bibliography

URLs are valid as of the publication date of this document.

[Alberts 2004]
Alberts, Chris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU/SEI-2004-TR-015 ADA453378). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.cert.org/archive/pdfs/04tr015.pdf http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html.

[Bace 2001]
Bace, Rebecca & Mell, Peter. Intrusion Detection Systems (NIST Special Publication 800-31). http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (2001).

[Barker 2003]
Barker, William C. Guideline for Identifying an Information System as a National Security System (NIST Special Publication 800-59). http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf (2003).

[FFIEC 2002]
Federal Financial Institutions Examination Council (FFIEC). IT Handbook InfoBase. http://www.ffiec.gov/ffiecinfobase/index.html (2004).

[Grance 2004]
Grance, Tim; Kent, Karen; & Kim, Brian. Computer Security Incident Handling Guide (NIST Special Publication 800-61). http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (2004).

[Hash 2005]
Hash, Joan; Bartol, Nadya; Rollins, Holly; Robinson, Will; Abeles, John; & Batdorff, Steve. Integrating Security into the Capital Planning and Investment Control Process (NIST Special Publication 800-65). http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf (2005).

[ISF 2005]
Information Security Forum. The Standard of Good Practice for Information Security. 2005. http://www.isfsecuritystandard.com/.

[ISC2 2005]
International Information Systems Security Certification Consortium (ISC)2. Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). https://www.isc2.org/cgi-bin/content.cgi?category=97 (2004).

[ISO 2005a]
International Organization for Standardization. Information technology — Security techniques — Code of practice for information security management (ISO/IEC 17799:2005) http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612 (2005).

[ISO 2005b]
International Organization for Standardization. Information technology — Security techniques — Information security management systems – Requirements (ISO/IEC 27001:2005).http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103 (2005).

[ITGI 2006]
IT Governance Institute. Control Objectives for Information and related Technology (COBIT) 4.0. 2006. http://www.isaca.org/cobit.

[Killcrece 2002]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. CSIRT Services. http://www.cert.org/csirts/services.html (2002).

[Killcrece 2003a]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. State of the Practice of Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-TR-001, ADA421664). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. http://www.cert.org/archive/pdf/03tr001.pdf http://www.sei.cmu.edu/publications/documents/03.reports/03tr001.html.

[Killcrece 2003b]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. Organizational Models for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-001, ADA421684). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. http://www.cert.org/archive/pdf/03hb001.pdf http://www.sei.cmu.edu/publications/documents/03.reports/03hb001.html.

[Mell 2002]
Mell, Peter & Tracy, Miles C. Procedures for Handling Security Patches (NIST Special Publication 800-40). http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf (2002).

[NARA 2003]
The National Archives and Records Administration. General Records Schedule 24 – Information Technology Operations and Management Records. http://www.archives.gov/records-mgmt/ardor/grs24.html (2003).

[NIST 2004]
National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (2004).

[NIST 2005]
National Institute of Standards and Technology. Computer Security Expert Assist Team. http://csrc.nist.gov/cseat/ (2005).

[NIST 2006]
National Institute of Standards and Technology. Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200). http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (2006).

[NIST 2007]
National Institute of Standards and Technology. NIST Special Publications, 800 Series. http://csrc.nist.gov/publications/nistpubs/ (2007).

[OGC 2006]
Office of Government Commerce. IT Infrastructure Library (ITIL).

http://www.itil.co.uk/ (2006).

[OLRC 2003]
Office of the Law Revision Counsel, U.S. House of Representatives. United States Code, Title 44, Sections 3541-3549 "Federal Information Security Management Act of 2002." http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t43t44+1817+13++() (2003).

[OMB 1996]
Office of Management and Budget. Circular No. A-130, Revised, Appendix III, Security of Federal Automated Information Resources. http://www.whitehouse.gov/omb/circulars/a130 /a130appendix_iii.html (1996)
http://www.whitehouse.gov/omb/circulars/a130/appendix_iii.pdf (1996).

[Ross 2004]
Ross, Ron; Swanson, Marianne; Stoneburner, Gary; Katzke, Stu; & Johnson, Arnold. Guide for the Security Certification and Accreditation of Federal Information Systems (NIST Special Publication 800-37). http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf (2004).

[Sharp 2001]
Sharp, Alec & McDermott, Patrick. Workflow Modeling: Tools for Improvement and Application Development. Boston, MA: Artech House, 2001.

[SEI 2002]
Software Engineering Institute. Securing Networks Systematically — the SKiP Method. http://www.cert.org/archive/pdf/SKiP.pdf (2002).

[SEI 2003]
Software Engineering Institute. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). http://www.cert.org/octave/ (2003).

[SEI 2005]
Software Engineering Institute. Capability Maturity Model Integration (CMMI). http://www.sei.cmu.edu/cmmi/ (2005).

[Swanson 1996]
Swanson, Marianne & Guttman, Barbara. Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST Special Publication 800-14). http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (1996).

[Swanson 1998]
Swanson, Marianne. Guide for Developing Security Plans for Information Technology Systems (NIST Special Publication 800-18). http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF (1998).

[Swanson 2001]
Swanson, Marianne. Security Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26). http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (2001).

[Swanson 2002]
Swanson, Marianne; Wohl, Amy; Pope, Lucinda; Grance, Tim; Hash, Joan; & Thomas, Ray. Contingency Planning Guide for Information Technology Systems (NIST Special Publication 800-34). http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf (2002).

[Wack 2002]
Wack, John; Cutler, Ken; & Pole, Jamie. Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41). http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (2002).

[West-Brown 2003]
West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition (CMU/SEI-2003-HB-002, ADA413778). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. http://www.cert.org/archive/pdf/csirt-handbook.pdf http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2007	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Incident Management Capability Metrics Version 0.1	FA8721-05-C-0003

6. AUTHOR(S)

Audrey Dorofee; Georgia Killcrece; Robin Ruefle; & Mark Zajicek

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2007-TR-008

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Successful management of incidents that threaten an organization's cyber security is a complex endeavor. Frequently an organization's primary focus on the response aspects of security incidents results in its failure to manage incidents beyond simply reacting to threatening events.

The metrics presented in this document are intended to provide a baseline or benchmark of incident management practices. The incident management functions—provided in a series of questions and indicators—define the actual benchmark. The questions explore different aspects of incident management activities for protecting, defending, and sustaining an organization's computing environment in addition to conducting appropriate response actions. This benchmark can be used by an organization to assess how its current incident management capability is defined, managed, measured, and improved. This will help assure the system owners, data owners, and operators that their incident management services are being delivered with a high standard of quality and success, and within acceptable levels of risk.

14. SUBJECT TERMS	15. NUMBER OF PAGES
incident management capability metrics, indicator, benchmark	229

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102